Bundesministerium
für Wirtschaft
und Technologie

Documentation
No. 581

Documentation

Internet of Things

A guide to technical, organisational, legal and safety-related aspects of implementing new RFID-supported processes in industry and government

www.bmwi.de

Editors:
Alfons Botthof, Institute for Innovation + Technology at VDI/VDE-IT GmbH (project lead)
Dr. Marc Bovenschulte, VDI/VDE Innovation + Technik GmbH
Dr. Sergei Evdokimov, Humboldt-Universität zu Berlin
Dr. Benjamin Fabian, Humboldt-Universität zu Berlin
Peter Gabriel, VDI/VDE Innovation + Technik GmbH
Prof. Dr. Oliver Günther, Humboldt-Universität zu Berlin
Prof. Dr. Ernst A. Hartmann, Institute for Innovation + Technology at VDI/VDE-IT GmbH

Production/Printing
Harzdruckerei GmbH Wernigerode

Published by
Federal Ministry of
Economics and Technology
Public Relations Division
10115 Berlin
www.bmwi.de

Last revised
May 2009

Zertifikat seit 2002
audit beruf**und**familie

The Federal Ministry of Economics and Technology (BMWi) has received the berufundfamilie® audit certificate for its family-friendly HR policy. This certificate is conferred by berufundfamilie gGmbH, an initiative of the Hertie foundation.

Bundesministerium
für Wirtschaft
und Technologie

Documentation

Internet of Things

A guide to the technical, organisational, legal and safety-related aspects of implementing new RFID-supported processes in industry and government

Executive summary

Increasingly, RFID technologies are becoming the method of choice for identifying all types of objects, in addition to barcodes.

The efficient processes, new products and innovative services we have today owe much to the ability to clearly identify objects and make information related to those objects available at any time and location. Fitting these objects with sensory capabilities and location identification functions, using GPS for example, **also enables autonomous, quasi-intelligent applications** that can incorporate networked object-to-object communication **(smart, interacting objects).** All of these applications, which are based on deployment of current and future identification technologies, essentially depend on **communication and database access** that offers reliability, security and integrity. Information and communication technologies must fully meet these demanding requirements, particularly when data are transferred in open networks that are exposed to external risks. This challenge must be met if the technology is to gain the acceptance required for their successful introduction and win the trust of customers, subscribers and users in industry and society.

The study presented here, commissioned by the Federal Ministry of Economics and Technology (BMWi), highlights the main **technical procedures involved in organising superior, Internet-based communication processes for the Internet of Things**.

Focusing on the topic of the ONS (**O**bject **N**aming **S**ervice) (management of and access to a basic directory of object identifiers plus querying of decentralised descriptive data) as an example, the study does not attempt to cover in detail questions of governance regarding the future infrastructure of an Internet of Things (administrative autonomy, data protection and rights of data subjects).

▸ **The study draws the attention of managers, especially IT managers in companies, to the technical, organisational, legal and safety-related aspects of implementing identification technologies and also to their implications. Valuable tips and suggestions are provided on the secure implementation of RFID-based processes (i.e. ensuring reliability and integrity), in IT solutions today. Recommendations drawn from expert discussions with stakeholders are addressed at those responsible for driving innovation within the field.**

If **business leaders are to work together with partners in the value-added process and move successfully towards an Internet of Things**, they must be aware of the key information and communication processes that can be enabled by introducing the RFID technology into products, processes and associated services. These guidelines are intended to provide key information about the technology, while outlining related opportunities and limitations.

Summary[1] of views

Current status	Future developments
Barcode (2D) RFID systems (readers, labels), occasional use of RFIDs with integrated sensor technology	Barcode (2D, 3D) More self-powered, network-enabled RFID labels with sensor functions
IPv4	IPv6
Centralised intermediary (ONS) between object code and (product) information databases	Decentralised organised services (regional ONS architectures, peer-to-peer architectures)
Unipolar ONS	Multipolar ONS
EPCglobal network (mainly for retail)	EPCglobal and other branch-specific networks
Uniform EPCglobal standard, guarantee of unique assignment of EPC numbers	Sector-specific additional standards, unique assignment of EPC numbers retained
Low scalability of the ONS	High scalability of the ONS
IT risks (e. g. data integrity, data authenticity, data availability, data confidentiality)	New procedures for reducing IT risks and improving IT security
Centrally organised and managed global security infrastructure	Decentralised organised and managed security infrastructure
Lack of consistent strategy at a European level on future power structures and governance	ONS that is industry and technology neutral; European agreements on governance structures
Inadequate transparency regarding technical and political developments related to the „Internet of Things“	Established Internet of Things/Services watchdog body acting on behalf of German stakeholders
German interests poorly represented within international standardisation bodies; no neutral standards	Nationally agreed standardisation strategy and structures representing SME interests
Mainly abstract cooperation on future infrastructure	Cooperation on infrastructure based on the requirements of specific projects
Little strategic importance for businesses (especially SMEs) (clinging to familiar solutions; with the exception of retailers)	High operational and strategic potential Replacement of outdated EDI structures
Businesses affected are not adequately prepared for the challenges and opportunities created by the introduction of the ONS	Extensive publicity measures supported by a large number of stakeholders
Little familiarity with „use cases“ for ONS	Empirical values derived from sector-specific, best-practice solutions
Lack of clarity about cost-benefit situation	Use cases with sample calculations to help guide users
High costs for services due to near monopoly of structures	Lower costs due to competition
Basic, inflexible payment model	Ubiquitous billing system (micro-payment per data access or read event)
Difficult to build customer profiles in „closed loops“	Simpler profiling in open processes that include the end customer

[1] These evaluations were provided by a group of subject experts (see list on page 52) who took part in extensive interviews as part of the study.

We would like to thank all representatives from science and industry who participated in the study for their willingness to contribute to the discussion on the ONS (quite intensively in some cases) and for making themselves available for our extensive interviews. We also extend our thanks to the members of the German RFID roundtable for their constructive suggestions.

Contents

1. Introduction, study objective and design

During the course of accompanying research conducted for the programme NextGenerationMedia of the German Federal Ministry of Economics and Technology, it became clear that the topic of RFID and the much hailed advance towards an „Internet of Things“ and „Internet of Services“ were closely linked to the EPCglobal Network and Object Naming Service (ONS). The ONS is used as a basic directory for assigning the ID (identifier) stored in the RFID tag with related stored information. For EPC (Electronic Product Code), the definitive technology within the retail and consumer goods sector, the ONS is operated by the company Firma VeriSign in the US, on behalf of GS-1/ EPCglobal. Using the existing operator model, international access to data that is addressed via RFID occurs centrally through a server based in the US.

Political, scientific and industry representatives have repeatedly expressed reservations about this type of centralised (monopolised) infrastructure and the dependency it causes. The risk of possible abuse associated with centralised control of goods and information flows, such as access to confidential logistics data threaten fair competition. There are particularly grave concerns in the case of data associated with state sovereignty (e.g. space travel, defence sector) rather than electronic product codes for consumer goods. The view is that management of data streams like these, which are critical for the state, should only be transferable to third parties in very limited circumstances to protect security, availability and exclusivity.

The subject of the ONS and the organisational structure of the Internet of Things are becoming increasingly important: at present, the question of ensuring state sovereignty and infrastructural security is still unresolved. Meanwhile the first European EPC Root ONS in Europe is being installed in France.

It remains to be seen whether the future Internet of Things will undergo a development similar to the transformation of today's Internet with WWW and HTML. In the future, we expect to have appropriate services for allocating or querying identifiers, and enabling all private Internet users to access new objects.

These models urgently raise the following questions: Who has access to which data? Who is authorised to save which data for which objects? How are the services on offer paid for? How can data sovereignty be ensured? How can the requirements for security, data protection and consumer protection be fulfilled?

The other development stages (key terms ONS 2.0 or IPv6, peer2peer) also require expert evaluation and careful consideration before new technical and organisational solutions are introduced for the Internet of Things and Services. These considerations should take account, in particular, of the role of IPv6 in the Internet of Things and identifying possible measures required. Concrete scenarios in potential user sectors will be useful in determining the sustainability of various measures from an organisational and security-related viewpoint.

This short study has been compiled, as part of the accompanying research conducted for NextGenerationMedia. It examines the possible influence and measures that can be exercised by industry and politicians regarding the technical design/implementation of this type of system and the creation of an appropriate framework. It is intended, in particular, to describe the current awareness of the above questions and report, by way of example, on the requirements of domestic industry.

The current study discusses these problems in an interdisciplinary context, with reference to the relevant technological, infrastructural, economic, legal and safety-related challenges. In addition to focusing on the current state of the ONS, it has amassed expert views through interviews with senior developers and users in the field of the EPCglobal Network/Internet of Things. Based on these views, it outlines the future shape of the ONS and alternative developments.

It is also important that we consider longer term developments within the framework of this study, to supplement the current initiatives in this field implemented by German businesses, which mainly focus on a two-year timeframe. After all, transforming the Internet of Things and Services from prototypical implementation to critical infrastructure will take a good five to ten years. A transformation of this type usually takes place in the form of spurts, rather than in a linear progression. Design decisions that are currently being made can have a sudden and damaging impact on this process. It is therefore crucial that these design decisions be evaluated now, against the current political and economic background.

In particular, we must ask whether additional political measures are required in relation to business interests or to safeguard German industry, following the project results of NextGenerationMedia. The study should help to represent and evaluate the interests of German industry through dialogue with academic and scientific experts; propose recommendations on governance; and bring about possible technology policy initiatives.

Even if the Internet of Things may not yet be uppermost among many companies' priorities, this type of initiative cannot be deemed premature. We do not need to ask whether the Internet of Things and Services will become a reality. This is an absolute certainty in the medium term. Rather the question is how to achieve an Internet of Things and Services in the most efficient way possible: one that offers maximum overall benefit to the German and European national economies. With this in mind, the following actions are vital: We must view the ONS and the Internet of Things as a critical infrastructure that will play an important role in the future; we must conduct a thorough prior analysis of its impact on the reliability and security of national structures; we must also carry out a comprehensive evaluation of the infrastructure in terms of regulatory policy.

Chapter 2 provides a brief introduction to the ONS concept in the EPCglobal Network and the current discussions surrounding the Object Naming Service. The interviewees taking part in the study were given Sections 2.1 to 2.3 from this chapter before the discussion to introduce them to the topic and prepare them for the interview.

Chapter 3 analyses the current ONS specification in terms of technical, organisational and IT security challenges. The current alternative and complementary options such as multipolar ONS, Peer-to-Peer ONS and DNSSEC are also discussed. The interviews conducted with experts from industry and trade associations as part of this study are summarised in Chapter 4. Drawing on these analyses and interviews, Chapter 5 recommends measures to the Federal Government.

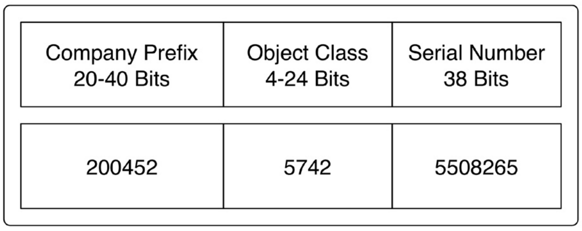
2. Introduction to the EPCglobal network and the ONS

2.1 Purpose of a naming service for the Internet of Things

The basic concept behind Radio Frequency Identification (RFID) is the association of physical objects with small, inexpensive computer chips (or *tags* as they are known) that can be scanned without contact or line of sight via radio waves.

The tags typically assign internationally unique identifiers to the objects associated with them. The most important convention for these identifiers is the *Electronic Product Code (EPC)* defined by the EPCglobal industry consortium. EPCs are used in a numbering system for naming objects that is internationally unique and globally available. An example of an EPC is shown in Fig. 1.

Figure 1: Example of an EPC



Company Prefix 20-40 Bits	Object Class 4-24 Bits	Serial Number 38 Bits
200452	5742	5508265

The first part (*Company Prefix*) indicates which company produced the object in question. The second part (*Object Class*) indicates the type of object (e. g. a particular item of clothing). The third part (*Serial Number*) is a key innovation over the conventional barcode. This series number is used to differentiate between different instances of the same product class, such as different trousers from the same manufacturer in the same style and size.

In general, product and logistical data for a concrete object are saved to networked database systems belonging to different logistics partners rather than directly to an RFID tag, with the EPC used as a search key for information. These databases may be distributed internationally and accessed via the Internet as *EPC Information Services (EPCIS)*. Combined with other services, this global information architecture is also known as the „Internet of Things“. As such, it serves as a precursor to and future extension to an Internet comprising directly linked „Smart Objects“ (for example, based on the IPv6 protocol).

The international industry consortium *EPCglobal* is the main driver behind standardisation of the EPC and related information architectures, and plans to operate a specific, commercially driven version of the Internet of Things with its *EPCglobal network*.

How do we get from an EPC, i.e. a unique identifier for an object, to the related object-specific information, or more particularly, to the relevant EPC information services? This is the task of naming and lookup services such as the *Object Naming Service (ONS)* and (*Discovery Services*). Highly detailed specifications are already available for the ONS: a thorough analysis of these is provided in this study. As yet, no such detailed specifications are available for the discovery services.

2.2 How the Object Naming Service works

When you use an RFID reader to scan the EPC of an object, access to the object-relevant information is not yet available. For this purpose, you must locate and consult the relevant information services (EPCIS) on the Internet. The ONS provides the necessary procedure for „resolving“ EPCs into Internet addresses of the relevant EPCIS (in the form of URLs).

ONS can be envisaged as a distributed, hierarchically organised information system. The highest level of the hierarchy (*ONS Root*) contains the addresses of the nodes on the second level (EPC Manager) that are operated by producers or wholesalers, for example, and are responsible for a particular range of EPCs. The EPC Managers for their part contain the addresses of EPCIS representing interfaces to databases where the relevant product and logistics data are saved.

Figure 2: Query process in ONS

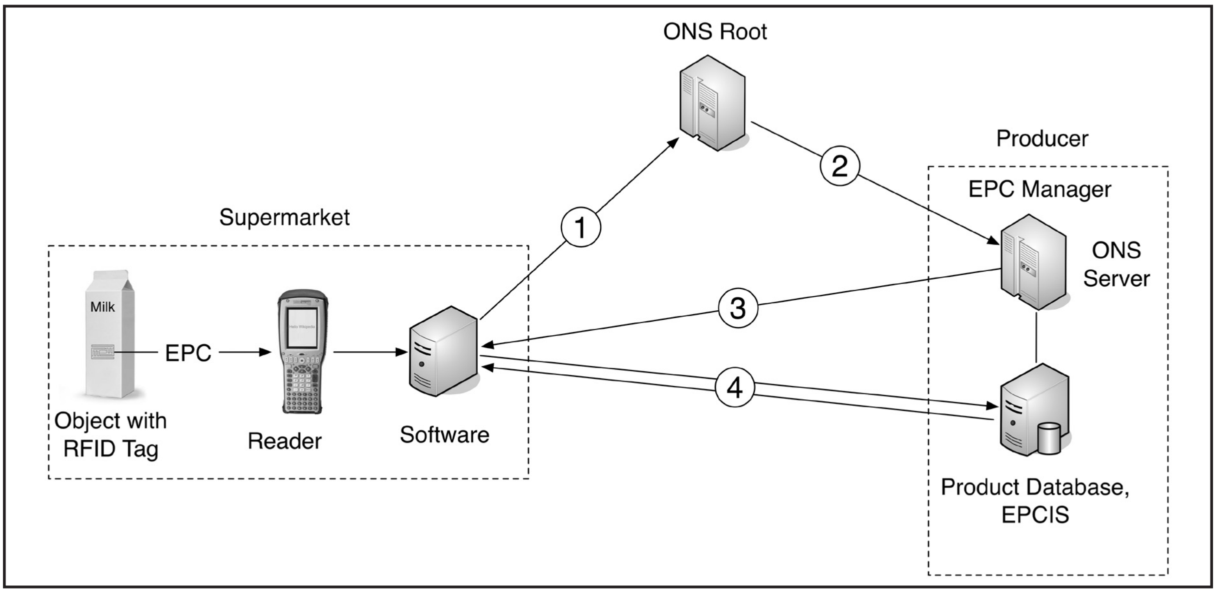


Figure 2 illustrates a simplified sample scenario. An RFID tag attached to a milk carton is scanned in a supermarket. To extract the relevant data for the milk carton concerned from the „Internet of Things“, special software (middleware) is used to send the query to the ONS root (step 1). The ONS root delegates the query to the ONS root of the EPC Manager, i.e. to the ONS infrastructure of the company that produced the milk carton (and/or the milk it contains). This is step 2. The EPC Manager's assigned ONS server (or servers) returns the Internet addresses of the EPCIS that could contain relevant product data to the querying party (Step 3).

Using these addresses, the product and logistics data for the scanned EPC can be requested from the EPCIS, although access restrictions may be applied (Step 4).

The addresses of the relevant ONS server or even of the EPCIS may already be known through caching of previous query results. In these cases, the ONS server or EP-CIS could also be contacted directly without involving the ONS root. However, if the cache does not yet contain the relevant addresses, or if the cache is no longer up-to-date, the query runs in the manner displayed in Figure 2.

2.3 Challenges facing the ONS

In 2008, over two billion RFID tags will have been sold. This figure is expected to grow to 500 billion by the year 2016.[2] The more companies and private individuals that use RFID, the more important the ONS will become as a global distributor of RFID information. It is therefore essential that the ONS has an efficient and reliable structure, and that it meets well defined fairness criteria.

An initial technical ONS standard has already been published and ratified by EPCglobal. However, given the important future role that the ONS (like the standard Internet) is likely to play in international transactions and the forecast greater dependency of national economies on the ONS, it is absolutely vital to evaluate this provisional ONS not only from a technical perspective, but also to assess its economic and political implications.

One of the main tasks of the ONS is to make a standardised path available to users working together in a value added chain, so that they may exchange a large volume of detailed information on the status and movement of goods. In the medium term, this can lead to major efficiency gains in today's ubiquitous complex value added chains, especially since transparency in processes and the flow of goods can be leveraged to improve planning and optimise logistical processes. We do not need to ask whether the Internet of Things and Services will become a reality. This is an absolute certainty in the medium term. Instead, we need to ask ourselves how to achieve an Internet of Things and Services in the most efficient way possible: one that offers the maximum overall benefit to the German and European national economies.

Before these forecast efficiency gains can be achieved, a number of obstacles must be overcome. These include the following:

- Uneven allocation of costs and benefits of an ONS infrastructure among the participants in a value added chain;;

- Relevant investments only become profitable in the medium to long-term and

- Risk of businesses becoming „locked-in“ if they become too dependent on the ONS - and thus also on EPCglobal's corporate strategies and on the companies commissioned with operating the ONS.

Bearing these considerations in mind, the following is vital: Germany and other countries must view the ONS and the Internet of Things as a future IT infrastructure; a thorough prior analysis of their effects must be conducted on the reliability and security of national structures; a comprehensive review of the regulatory aspects must be carried out.

ONS-internal power structures

The ONS root determines the EPC manager to whom the queries are sent. It acts as a critical intermediary in the global system, thus affecting the information search for all products worldwide. Since the EPC manager determines which of its own EPCIS can be located with ONS, its influence is restricted by comparison to the ONS root to information about its own products.

The as yet unspecified EPCIS Discovery Services should greatly support the search for any relevant EPCIS for an object (that is, independently of one operated by the particular manufacturer).

[2] Raghu Das and Peter Harrop, „RFID Forecasts, Players & Opportunities 2008-2018“, http://www.idtechex.com/research/reports/rfid_forecasts_players_and_opportunities_2008_2018_000193.asp.

Unipolarität

VeriSign, the main provider of the ONS root, is a company that is subject to US law, a factor that could possibly complicate matters for such a vital international infrastructure. It is not yet clear whether other countries will follow France's example (see. 3.1.1.2) and operate their own ONS roots, and how independent from VeriSign these would be in practice. Unresolved issues include coordination and data replication between the (numerous) roots and administration of the ONS root file, plus the ease of integrating alternative architectures for individual countries or regions.

Integrity

ONS uses the established DNS (Domain Name System) Internet protocol: This is used to send all messages in plain text and mainly on the basis of the stateless User Datagram Protocol (UDP), which, for reasons of speed, does not include any error identification or sequential numbers for messages. In practice, the DNS's own identification numbers for allocating queries and responses are not designed to prevent falsified communication or even falsification of DNS data on the servers in some cases.[3] Established attack models (e. g. man-in-the-middle attacks or cache poisoning) can thus simply be transferred to the ONS. There is no option in the current ONS specification that guarantees the integrity and authenticity of address data.

One of the proven concepts in IT security is the defence-in-depth principle, which places the maximum number of obstacles in the path of a potential attacker. Safeguarding data integrity should therefore not be assigned exclusively to the EPCIS communication (in any case, this would be inadequate): If you falsify the assignment of the EPC to the URL in the ONS, you are usually unable to tell that you have not contacted the correct communication partner for this EPC, e. g. by using the SSL/TLS certificate of the EPCIS, which can be correctly issued (but only proves the correct assignment of URL to identity).

Availability

The ONS root represents a „single point of failure“: In this day and age of „Bot“ networks consisting in some cases of hundreds of thousands of infected, remotely controlled computers, the small number of central ONS root servers (compared to the number in the overall system) must inevitably deal with massive, concentrated attacks via innumerable queries that can disrupt operation (distributed denial-of-service). Further research is required to determine whether current replication measures for the DNS can continue to cope with these new threats in the future.

Confidentiality and anonymity

Confidentiality of ONS data cannot be guaranteed on the basis of the DNS. Even if the actual EPCIS communication is authenticated and encoded, user queries to the ONS can simply be read and recorded, together with the original address (which can often be traced to a particular location or person) by all servers, the ONS root or by any Internet service provider. Each ONS query from a company or person refers to objects in the real world and could be used for identification, profile generation (assets, relationships) and finding the approximate location of the user. While disclosure may occur in less detail than with RFID data protection problems and RFID readers, it would be on a global scale with large user groups. The risk also applies to companies, whose logistics and procurement strategies could be accessed by third parties.

[3] This problem was also raised in the mass media in summer 2008, e. g. Leaks in Patch for Web Security Hole; NY Times, August 8, 2008: http://www.nytimes.com/2008/08/09/technology/09flaw.html or German article in Spiegel-Online of 7.8.2008, „Wie ein Riesenloch im Netz die Sicherheit bedroht“: http://www.spiegel.de/netzwelt/web/0,1518,570584,00.html; Last access 12.11.2008

2.4 Political issues concerning the ONS

The challenges posed by the EPCglobal Network and the ONS to economic and technology policies were recognised at an early stage. Two strands emerge from the political debate surrounding the ONS service: the first strand emphasises governance of the service, while the second focuses on the security of the service and the EPCglobal network.

Not long after the first formal ONS specification was announced in 2005 (updated in 2008 [EPC08]), the first groups of experts were already commenting on governance of the future ONS service. At a workshop held as part of the European Commission's RFID consultation process, Patrik Fältström (Cisco) referred to the risk of possible monopolisation of the EPC-global network by the ONS service operator [Fal06]. Within the academic arena, possible IT security risks associated with the EPCglobal network became the subject of research since roughly 2003, in for example the BSI study RFID – Security Aspects and Prospective Applications of RFID Systems ().

The subjects of governance and the security aspects of the ONS service entered the political discussion following the European Commission's communication *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* in March 2007 (EC 2007). Calls were made for integrated protection of privacy and IT security within RFID systems and concerns raised about the openness and neutrality „of the databases that will register the unique identifiers that lie at the heart of the RFID system". The commission set up a two-year RFID Expert Group to conduct an exchange between all relevant interest groups and help the commission define its RFID policies. The group mainly focused on devising a compromise solution for data protection in RFID systems. The results of the group's work have not yet been published. In addition, the Commission set up a number of research projects dedicated to the technical aspects of security within the EPCglobal network, in particular the BRIDGE project, which involves a number of GS1 organisations.

The topics of ONS governance and security were also examined in the study commissioned by the Federal Ministry of Economics and Technology titled *RFID: Prospectives for Germany* [BMWi07a]:. The results of the study were used as preparation for the BMWi Expert conference *RFID: Towards the Internet of Things*, held within the context of the German Presidency of the EU Council in 2007. For this purpose, the Federal Ministry of Economics in conjunction with the Federal Ministry of Research and the European Commission and a circle of German and European RFID experts drafted the position paper *European Policy Outlook RFID*. The paper proposed a series of recommendations for the widespread rollout of RFID applications and services [BMWi07b]. It also proposed a number of targeted activities to be undertaken by the European Commission in support of creating a decentralised and secure ONS service.

At the follow-up conference held during the French Presidency of the EU Council *Internet of the Future* in Nice in October 2008, the French government proposed setting up a European ONS service. A prototype of such a service was presented by French companies GS1 France and Orange France (a subsidiary of France Télécom). For the Nice conference, the Federal Ministry of Economics and Technology again raised the question of free access to all services and protection of confidential data in the Internet of Things with its follow-up paper to the *European Policy Outlook RFID* titled *Reflection Paper of the Federal Government of Germany*, [BMWi08] (see also 3.1.1.2).

Similar concerns were voiced by the European Commission in its working paper *Early Challenges regarding the „Internet of Things"*, which it had published to serve as up-to-date online reference. The paper proposes further consultation between member states, national data protection authorities and industry, in order to define minimum requirements for national governments regarding transparency (visibility) and control of critical components in the Internet of Things, necessary to protect the public interest [EC08].

3. ONS developments and outlook

Naming services for the Internet of Things are central to the global exchange of information in the Internet of Things. Technically, naming services are distributed systems that offer the following important lookup functions: You enter an identifier for an object, e. g. an electronic product code (EPC), and a list of Internet addresses for services is returned, giving you more information about the object. These services may take the form of EPC Information Services (EPCIS), whose communication protocols are also standardised by EPCglobal.

In addition to the EPC Object Naming Service (ONS) and alternative architectures for this basic function, work is also currently being carried out on extended lookup services such as the Discovery Services, which are designed to offer a comprehensive semantic framework for retrieving EPCIS, but are not currently standardised.[4]

Without this type of naming service and discovery services to act as intermediaries between objects and their related information sources, the Internet of Things could not attain the degree of flexibility and global scalability required to achieve its vision: that of radically changing the way information is processed in complex added value and logistics chains in production and commerce.

Easier retrieval of object-related information will enhance the transparency of value added processes.

The areas of application for these naming services can be subdivided into the following three groups:

- Production
- Logistics
- Private use

Production refers to transformation processes that create storable commodities or consumer durables from natural or manufactured raw materials. *Logistics* refers to processes involved in shifting commodities or consumer durables from one location to another. The entire value added chain is analysed, starting from the smallest supplier to the OEM (Original Equipment Manufacturer), who assembles the delivered components and sells them under a proprietary brand name. *Private use* refers to concepts of the future such as the intelligent house, intelligent office, personalised automated advisory services (e. g. nutrition advice, intelligent medical cabinet) in addition to applications in the health system.

Table 1 describes the advantages of naming services for these application fields.

Table 1: Advantages of naming services in various application fields

Application field	Advantages of naming service, e.g. ONS
Production	Efficiency gains in various production processes Simplification of global business relationships Flexible participation in value added chains
Logistics	Simplification of global business relationships Easier exchange of information about goods in global logistics networks Flexible participation in value added chains Increased transparency Efficiency gains Reduced costs Traceability of components and products
Private use	Simple product identification Traceability of products New services for intelligent office and home environments Support for advisory services

[4] See [BRI08]

To offer these advantages, a naming service for the Internet of Things must meet important requirements in various categories: the specific details of these requirements partly depend on future sample applications, e. g. whether or not there are real-time requirements for a response. Determining requirements in the iterative development process is therefore necessarily provisional and subject to revision.

Table 2: Requirements of a naming service

Category	Subcategories (examples)	Further specifications (examples)
Functionality	Supported participants Supported identification formats Type of information Publication function Query function	EPC: Object level EPC: Individual level (series number)
		Data on the object itself (e. g. „out-of-service“), in addition to address data?
Scalability	Number of participating providers and services Number of clients Number of EPCs and documents	„Low“ ($<10^4$) „Medium“ (10^5) „High“ ($>10^6$)
Performance	Response speed Server load	Response time < 1 h Response time < 10 s Response time < 1 s
Security	Availability Integrity Confidentiality	Confidentiality of address documents Confidentiality of query Anonymity of clients

In the following section, we first look at the precise architecture of the ONS, the official naming service in the EPCglobal network. We then present two sample ONS alternatives (MONS and OIDA), which differ especially in terms of the level of decentralisation and their inherent security mechanisms.

3.1 Object Naming Service (ONS)

To date, the Object Naming Service (ONS) has been the most influential proposal for a naming service architecture for the Internet of Things. The ONS was designed by the industry consortium EPCglobal [EPC08].

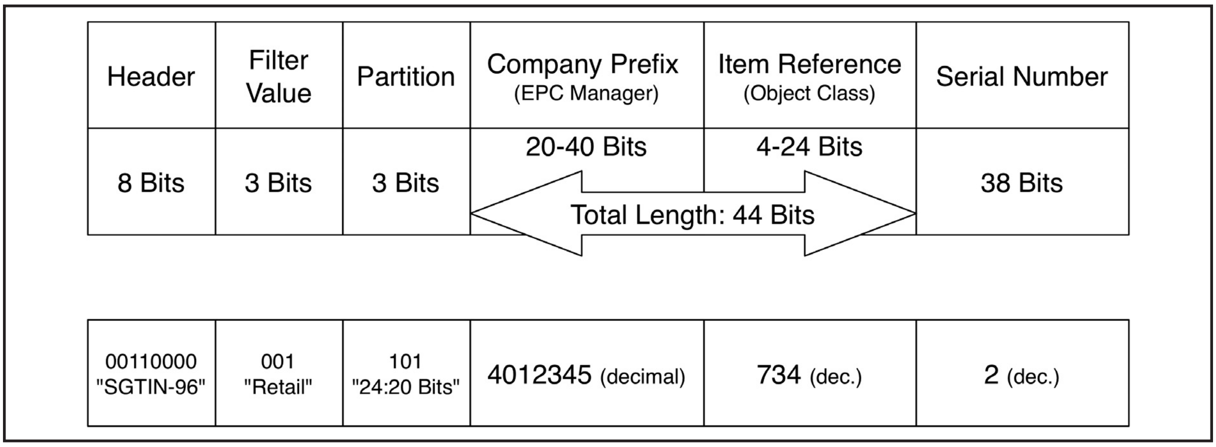
The following section describes the technology and organisation of the ONS and the associated challenges.

3.1.1 Technology and organisation

Every RFID tag that conforms with the EPC standard carries an EPC: this is used for unique, worldwide identification of the object bearing the tag. The EPC can thus be used as a unique search key for computerised tracking of an object and for exchanging object-related information. The EPC standard includes various namespaces and coding schemes: for example, for „Serialised Global Trade Item Number“ (SGTIN), „Serial Shipping Container Code“ (SSCC) und „Global Returnable / Individual Asset Identification“ (GRAI / GIAI).

As already mentioned, an EPC of the variant SGTIN-96, the successor to the EAN/UCC barcode, is subdivided structurally into the following segments (Figure 3: EPC Variant SGTIN-96): „Header“ (EPC type, SGTIN-96 in this case), „Filter Value“ (general object type for logistics), „Partition“ (auxiliary field for variable length of the two following values), „Company Prefix“ (also „EPC manager“), „Item reference“ (also „Object Class“, specific object type) and „Serial Number“ (unique serial number, together with the other segments). For ONS, the Company Prefix (EPC manager) and Item Reference (Object Class) are particularly relevant, in line with the previous specification. Assigning unique numbers means that object-related information can be managed separately from the object on servers on the Internet. Services (EPCIS) that are associated with an EPC can be located using the ONS, and these can then be used in turn to find information about a particular object.

Figure 3: EPC variant SGTIN-96



3.1.1.1 ONS Architecture

The EPC network allows flexible integration of several different parties (manufacturers, suppliers, logistics companies, supermarkets) into the infrastructure of the network.[5] Each party can make available information they have compiled about a particular object via information services and register this information dynamically within the network. Given the dynamic nature of this global network, static lists with object-

[5] See [EPC07]

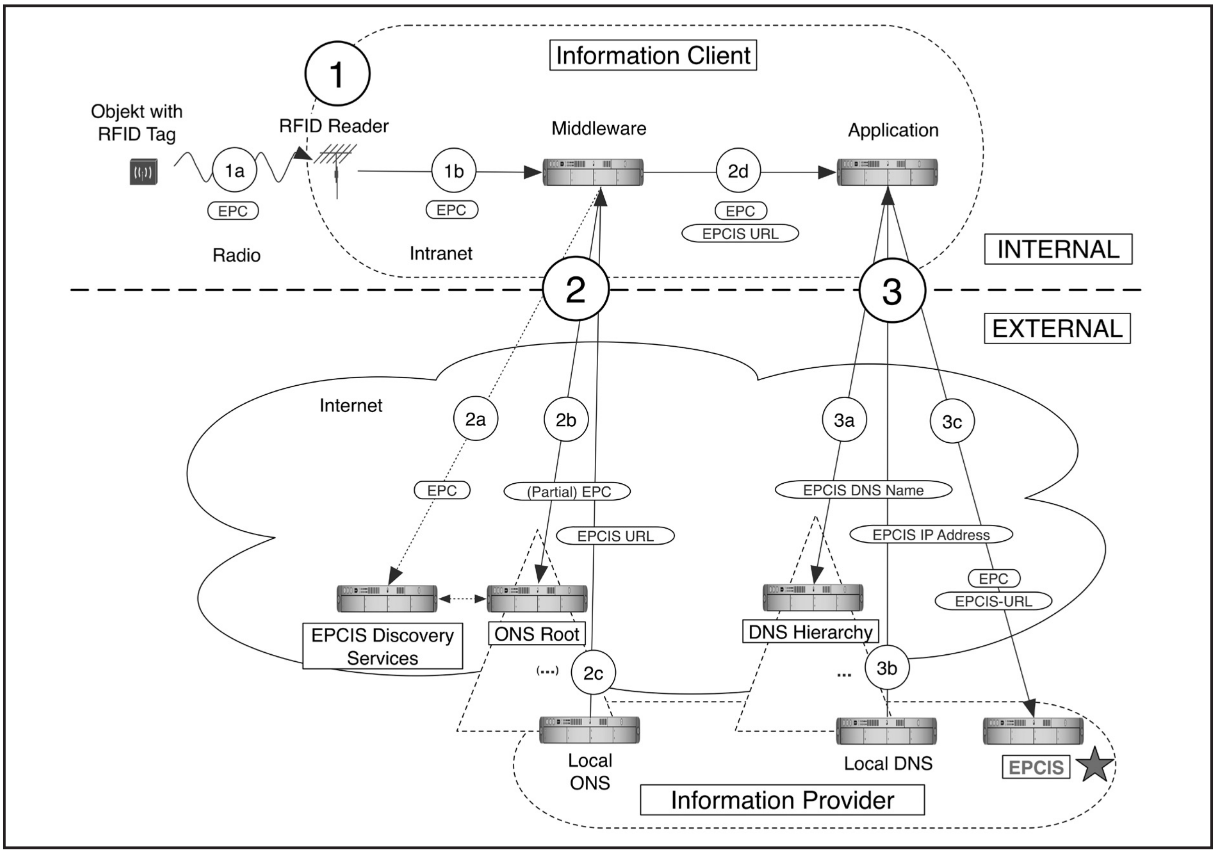
related data sources would quickly become obsolete. To obtain a current list of the relevant data sources, you can first query the ONS for each information search. For queries about an EPC, the ONS returns an up-to-date list with information services for the relevant object. However, the current plan is for this to include only information services from the object manufacturer, which will restrict the organisational functionality of the system. A full range of information sources is planned for the EPC Discovery Services, not yet released.

Technically, the ONS is based on the Domain Name System (DNS). This is based on the concept of translating an EPC into a syntactically correct domain name and using the existing DNS infrastructure, software and protocols to search for additional information.[6]

To locate information sources for an EPC, you generally need the addresses (usually in the form of DNS names) from EPCIS for the particular object.

In an interim step, an application or middleware first converts the EPC to a URI (Uniform Resource Identifier). The binary-coded SGTIN 47400.11015.473201 (decimal) contained in the original EPC is thus converted to the character string „urn:epc:id:sgtin:47400.11015.473201“. This character string is then converted by the actual ONS resolver to a domain name (e. g. „47400.11015.sgtin.id. onsepc. com“). Under the current ONS specification, the serial number section of the EPC (473201 in the example) is not included in the corresponding domain name, but space is explicitly provided for appropriate future extensions.

Figure 4: Communication flow in the EPCglobal network



[6] See [EPC08]

The DNS name thus created belongs to the domain onsepc.com, which is especially reserved for ONS. If the server (usually local) queried by the client does not have an entry for this name from an earlier query process (caching), a new query is sent to the ONS root (step 2 in Figure 4), using the standard DNS protocol. During this process, at least some parts of the queried EPC (at least the company prefix and item reference) are sent in plain text via the Internet, as these are an inherent requirement for delegating search requests. In future, discovery services will also be contacted during this step (step 2a).

The ONS returns the EPCIS addresses of the manufacturer that are relevant to the requested EPC. These addresses are available as conventional URLs, i.e. they contain DNS names that must be resolved via the standard DNS into IP addresses (step 3a), before the actual EPCIS can finally be contacted and information retrieved (3b).

3.1.1.2 Power structure

This technical process – combined with the architecture decisions of EPCglobal – creates a number of political and security-related challenges. VeriSign, the main ONS root provider, is a company that is subject to US law, something that could possibly complicate matters for such a vital international infrastructure. This unilaterally centralised architecture was the subject of much controversy. Eventually it led to the development of an independent ONS root server, which is operated by the French company Orange on behalf of GS1 France.

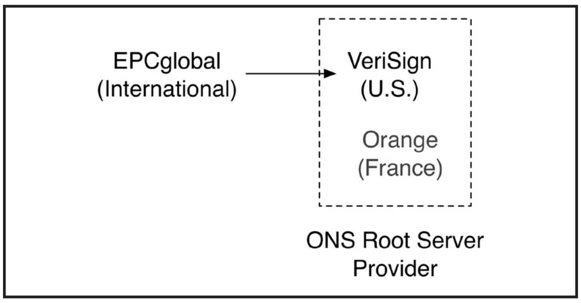
Since there is no agreement between EPCglobal and GS1 France regarding the interoperability of the root servers, GS1 France set up a work group to design a new ONS architecture that would support several independent ONS roots. The work group comprises employees from GS1 France, AFNIC (registry for .fr domain names), Afilias (registry for .info and.aero domains and service providers for the .org domain), INRIA (Institut national de recherche en informatique et en automatique), the Institut für Wirtschaftsinformatik (Institute for Information Systems) at the Humboldt-Universität zu Berlin and the Institute for Pervasive Computing at the ETH Zurich University.

This group is currently evaluating and standardising several ONS architecture proposals. The final architecture proposal is to be submitted by GS1 France to EPCglobal as a change request for the ONS Standard.

It is not yet clear whether other countries will follow France's example and operate their own ONS roots, and how independent from VeriSign these would be in practice. Unresolved issues include the number and coordination of roots, plus data replication between the roots and the administration of the ONS root file, in addition to the ease of integration of alternative architectures for individual countries or regions.

The ONS root decides which EPC manager is to receive the query. The EPC manager determines which EPCIS can be located with ONS. The as yet unspecified EPCIS Discovery Services should be very helpful in searching for any relevant EPCIS for an object (that is, independently of one operated by the particular manufacturer).

Figure 5: Power structure of the ONS



3.1.1.3 Economic aspects

Table 1 shows the advantages of the ONS and discovery services for various application fields. Clearly, manufacturing companies benefit least from these services, while simultaneously bearing the lion's share of costs for the provision and maintenance of the EPCglobal architecture concept and for the naming service (especially EPCglobal charges, provision of EPCIS and costs of RFID tags).

The unfairly distributed incentives could severely stunt the development of the Internet of Things where, after the EPCglobal architecture[7], naming services play a central role.

In cases where RFID is also used for production stages, where the costs of RFID tags can be disregarded and where the EPCIS is deployed and maintained by the party that benefits most from it, the manufacturer still has to order and pay for the relevant EPC number ranges. However, since there is no incentive for manufacturers to do so, they could potentially transfer these costs to parties who have a direct interest in the object naming services. These parties could incur significant costs as a result.

3.1.2 Security

The DNS is a standard, centralised Internet service with a long history of security problems, both within its own protocol and in its specific implementations. Many of the DNS's weaknesses occur because the service, which must be generally accessible at all times, is used for countless applications, but does not include any authentication mechanisms. Neither the queried server nor the information it holds can be authenticated via the DNS protocol. Furthermore, the entire communication occurs via plain text.
Of course, since the ONS is based on the DNS, these weaknesses are copied directly over to the ONS.[8]

3.1.2.1 Integrity

Ensuring the integrity of information from the ONS is problematic. It requires that all data maintained via the ONS is accurate and complete. Attackers can plant falsified data into the query results using standard ONS servers, ONS servers controlled by a system intrusion, or man-in-the-middle attacks on the communication process. For example, addresses of EPCIS that are controlled by an attacker may be inserted in the list. If these unauthorised actions are not prevented by authentication mechanisms, attackers can supply falsified information for the queried object or for many other objects from this domain.

As use of the EPC network becomes more widespread, its services are bound to be accessed by an increased number of applications. This applies for applications in the areas B2B and B2C and within the private sphere. The primary goal is to integrate the ONS in core business processes. These applications would urgently require reliable solutions for looking up object-related data sources. ONS uses the established DNS (Domain Name System) Internet protocol: This is used to send all messages in plain text and mainly on the basis of the stateless User Datagram Protocol (UDP), which, for reasons of speed, does not include any error identification or sequential numbers for messages.

In practice, the DNS protocol's own identifier numbers for assigning queries and responses are ill equipped to prevent third parties from falsifying communication or even in some cases the DNS data on the actual servers. In summer 2008, the problem was also aired in the mass media.[9] Basic gaps in DNS data authentication and in many established DNS servers were highlighted.[10]

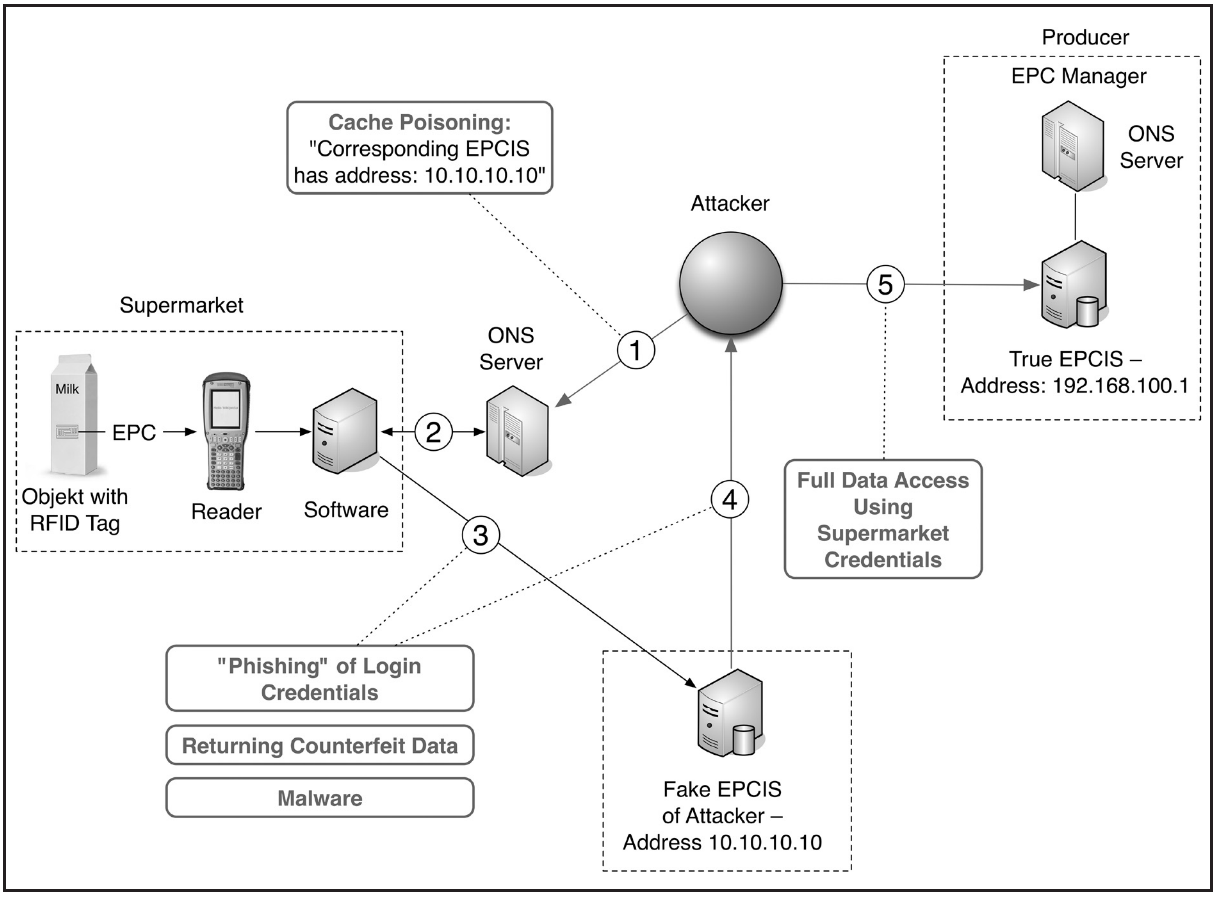
[7] See [EPC07]

[8] See [FGS05], [FG09]

[9] e. g. Spiegel Online from 7.8.2008, „Wie ein Riesenloch im Netz die Sicherheit bedroht“: http://www.spiegel.de/netzwelt/web/0,1518,570584,00.html (10/2008).

[10] See US-CERT http://www.kb.cert.org/vuls/id/800113 and the home page of DNS researcher Dan Kaminsky: http://www.doxpara.com/?p=1162 (10/2008).

Figure 6: Sequence of a cache poisoning attack


Producer
EPC Manager
ONS Server
Cache Poisoning: "Corresponding EPCIS has address: 10.10.10.10"
Attacker
5
Supermarket
ONS Server
1
True EPCIS – Address: 192.168.100.1
Milk
EPC
2
Objekt with RFID Tag
Reader
Software
4
3
Full Data Access Using Supermarket Credentials
"Phishing" of Login Credentials
Returning Counterfeit Data
Malware
Fake EPCIS of Attacker – Address 10.10.10.10

These established attack models, e. g. man-in-the-middle attacks or cache poisoning can simply be transferred to the ONS, since the software and protocol are directly based on the DNS. There is no option in the current ONS specification that guarantees the integrity and authenticity of address data.

If the ONS lacks data integrity, attackers can systematically redirect lookup requests to any number of targets, e. g. to EPCIS servers controlled by them. This type of cache poisoning attack is briefly outlined here (Figure 6):

1. An attacker manipulates the address inputs on any chosen ONS server, e. g. with information stating that the EPCIS for a product is available at another IP address (10.10.10.10 instead of the correct 192.168.100.1 address in the example). Established attack programmes are available for this purpose: they work by exploiting the weaknesses of the DNS server programs and the DNS protocol.[11]

2. Later, a standard client contacts the ONS server with a request, expecting a correct response. However, the server returns the manipulated address information (10.10.10.10) to the client instead, (a fact not recognised by the client).

3. The client now connects to the EPCIS on 10.10.10.10. This can result in numerous follow-on risks:

[11] For example, as a plugin for the established metasploit framework: http://www.metasploit.com/.

In the simplest case, the client does not receive any of the required information about the queried EPC. As a result, the relevant application may be unable to function correctly (denial of service).

As a web service, the falsified EPCIS can try to infect the client software with malware (viruses, backdoors, bot-software), in the same way as malicious servers exploit security gaps in a browser (i.e. web client) during standard Internet surfing.

The attacker can attempt to output its EPCIS as correct. The attempt may be successful if, for example, further security measures are either not available or ignored for the EPCIS connection (e. g. warnings about forged SSL certificates). In this case, the attakker can return all types of forged product information to the client. From here, the information can infiltrate the business processes. The EPCIS can also intercept the correct login data of the client and gain access itself to the correct EPCIS and obtain the information there (see steps 4 and 5 in the figure).

Insufficient measures ensuring integrity and authenticity in the ONS can thus result in many indirect risks, depending on the application field and the configuration of additional protective measures.

Table 3: Risks caused by inadequate protection of integrity

Application field	Indirect risks caused by insufficient integrity and authenticity in the ONS
Production	Restricted functionality Halt to production Sabotage Industrial espionage
Logistics	Restricted functionality Falsification of object data Manipulation of processes Data loss Industrial espionage
Private use	Falsification of product data Restricted or falsified functionality of services for intelligent office and home environments Restricted or falsified functionality of advisory services Spam

In addition, securing the ONS must take into account that the address data stored there also use DNS names for servers. Providing adequate security measures for the ONS requires that the DNS entries used must also be protected by authentication measures such as DNSSEC (see section 3.4 below).

3.1.2.2 Availability

The ONS will be exposed to a high volume of attacks from the Internet, since its very nature means it must be accessed by a large number of users. Relatively centralised, the ONS root is only distributed across a few servers - this in particular represents a single point of failure. It entails risks such as distributed denial-of-service (DDoS) attacks (see Figure 7). In the event of DDoS attacks, individual servers or their Internet connections are overloaded by a high number of artificially generated, parallel queries performed by a huge number of „bots“ (normal computers that are infected with malware unknown to their owners or regular users).

Alternatively, attackers can use special software errors to deactivate or remotely control the targeted service by means of attack programs („exploits“ programs that take advantage of security gaps).

A particular type of attack on availability can be made by taking control of the ONS root or all network connections leading to the root. This root blocking as it is known, can be used to block selected queries from particular countries, or even from particular clients, while other queries are answered as normal. This attack can lead to a virtual embargo situation, with a country being systematically excluded from using the ONS. If use of the Internet of Things grows and if its search functionality is deployed in vital business processes, a root blocking attack could be an effective means of attacking the critical infrastructure of a state.

Figure 7: Sequence of a distributed denial of service attack

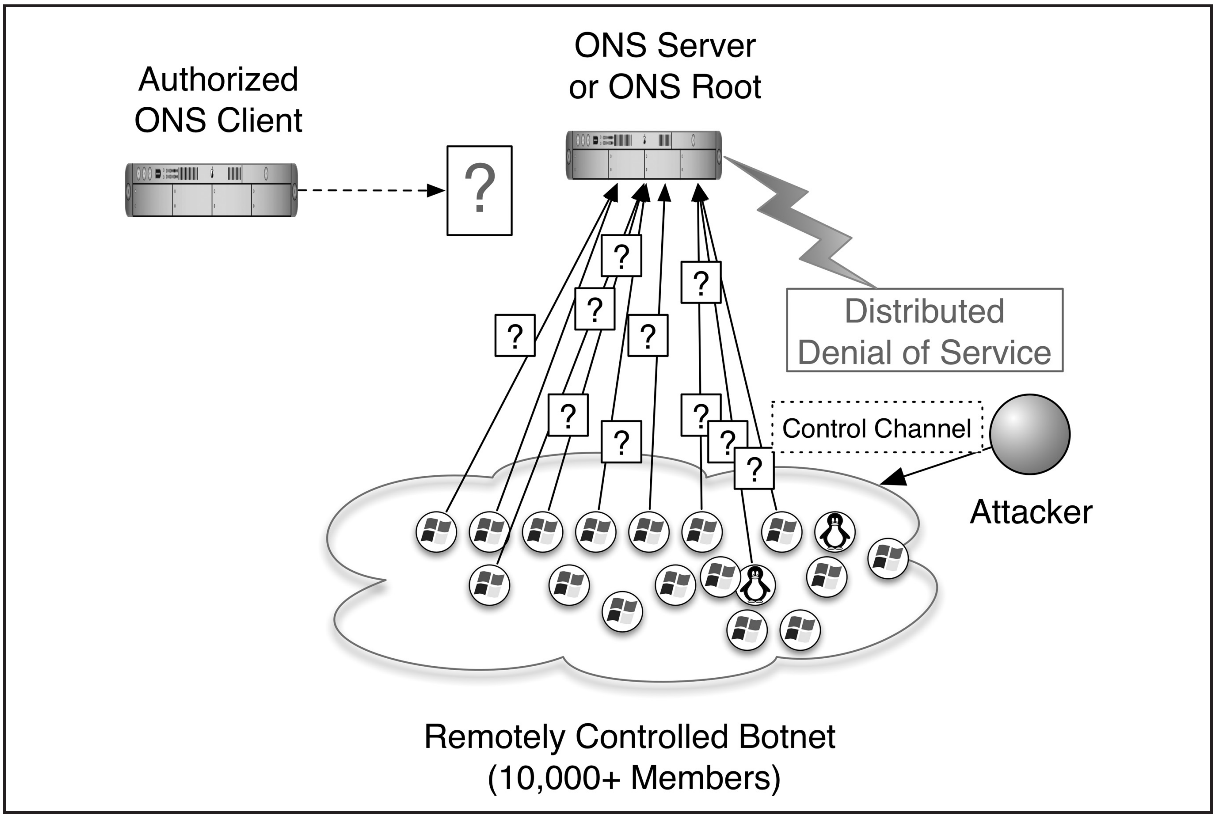


Table 4: Risks caused by inadequate protection of availability

Application field	Risks caused by insufficient availability
Production	Restricted functionality Halt to production Sabotage
Logistics	Order and delivery problems Prevention of status updates Restricted functionality Sabotage Reduced transparency
Private use	Unavailable product data Restricted functionality of services for intelligent office and home environments Restricted functionality of personalised advisory services

3.1.2.3 Confidentiality and anonymity

In many contexts, the EPCs on RFID tags and the related query behaviour within the Internet of Things could be categorised as sensitive information, especially if it can be gathered without any great effort and systematically evaluated using data mining procedures.[12] For example, an analysis of goods and material flows can supply valuable information about competitors and thus influence price negotiations. It is also relatively easy to link personal data with an EPC. This would make information available on the location and profile of individuals.

Even if the serial number section of the EPC cannot be recognised via the Internet, the combination of Company Prefix (manufacturer) and Item Reference (object class) can be used to identify the type of object to which the EPC belongs. Clusters of partial EPCs can be substituted for a complete EPC and become a unique key to connect objects with people or companies. Interaction with the actual EPCIS can also enable informative conclusions to be drawn about the object.

There have already been many proposals for preventing potential abuse. The main procedures proposed are those that protect the EPC on the tag from unauthorised scanning. However, the communication processes, which, like use of the EPC network, only occur after the actual RFID scanning operation, have been largely neglected to date.[13]

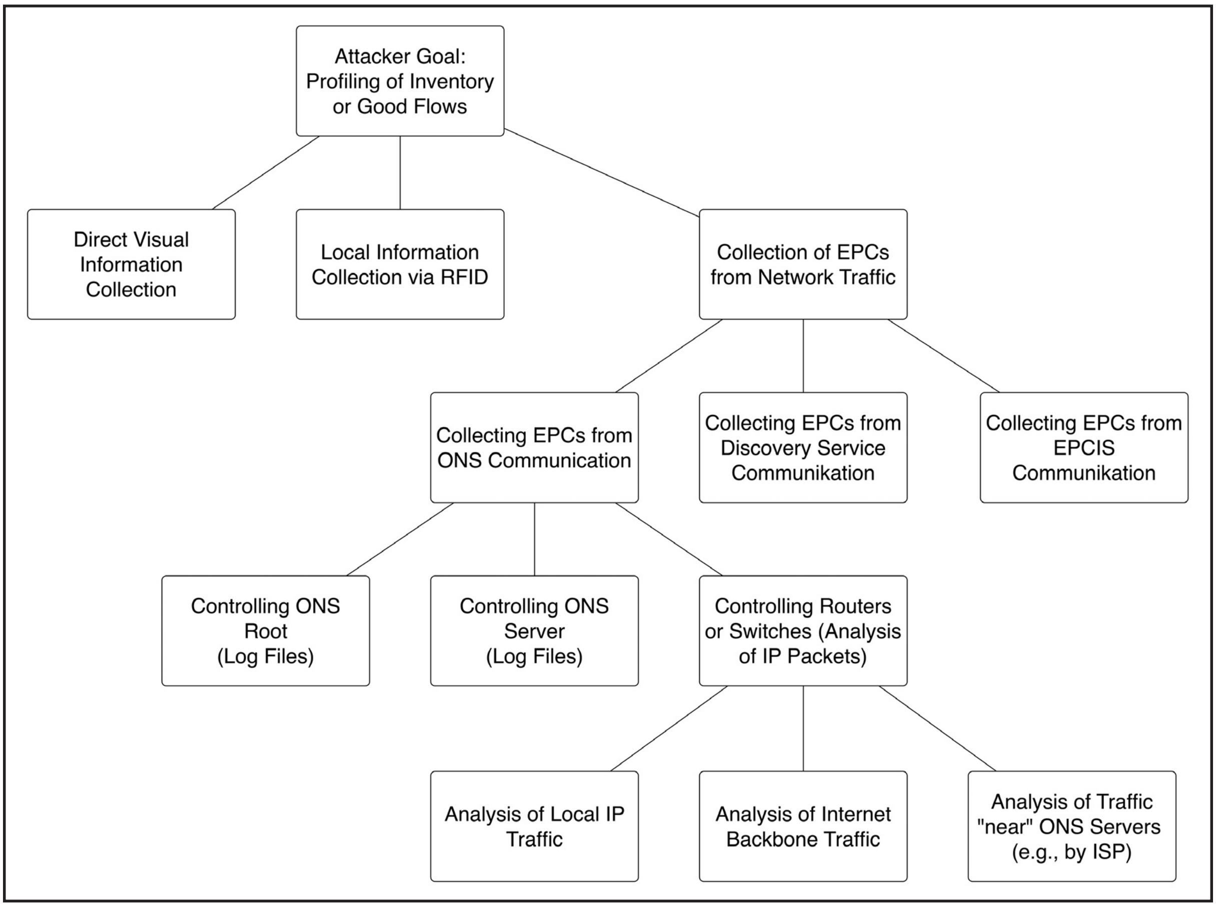
Before information belonging to an EPC can be retrieved from the EPC network, the corresponding EPCIS must be located via the ONS. Therefore, at the start of the process, unencrypted communication with the ONS takes place (if the address sought does not happen to be contained in a temporary local cache already). This occurs even if the connection to the actual data source (EPCIS) is subsequently set up in encrypted form (e. g. using SSL/TLS). The main section of the EPC is thus encoded for the DNS and sent to a DNS server in plain text. During this process, the information passes through the local network, which may be provided by a WLAN. If proper security measures are not in place, eavesdropping of network traffic can easily occur.

[12] See [GS05]

[13] See [FG09]

Depending on the cache and the configuration of the consulted DNS server, the query is routed along the pathfor name resolution in the DNS. The request may then be transferred to a root DNS server, onward to the assigned server for onsepc.com at VeriSign and possibly to other servers from the DNS or ONS hierarchy, until it reaches the company acting as the main reference for the queried EPC.

Figure 8: Profile generation strategies based on goods flows


Attacker Goal: Profiling of Inventory or Good Flows
Direct Visual Information Collection
Local Information Collection via RFID
Collection of EPCs from Network Traffic
Collecting EPCs from ONS Communication
Collecting EPCs from Discovery Service Communikation
Collecting EPCs from EPCIS Communikation
Controlling ONS Root (Log Files)
Controlling ONS Server (Log Files)
Controlling Routers or Switches (Analysis of IP Packets)
Analysis of Local IP Traffic
Analysis of Internet Backbone Traffic
Analysis of Traffic "near" ONS Servers (e.g., by ISP)

All Internet service providers whose networks are used to carry these types of queries can eavesdrop on parts of the queried EPCs. The same applies to authorities in the countries through which the data are routed. This opens up new opportunities for attackers who want to benefit from the analysis of the EPC-relevant data traffic (Figure 8).

Confidentiality of ONS data cannot be guaranteed on the basis of the DNS protocol. Consequently, queries from users sent to the ONS can be read by all servers, the ONS root or any Internet service provider and logged, together with the source address (can often be traced directly to a person). Each ONS query from a company or person refers to objects in the real world and could be used for identification, profile generation (assets, relationships) and finding the approximate location of the user. While disclosure may occur in less detail than with RFID data protection problems and RFID readers, it would be on a global scale with large user groups. This risk also applies to companies, whose logistics and procurement strategies could be accessed by third parties.

Table 5: Risks caused by inadequate protection of confidentiality

Application field	Risks caused by insufficient confidentiality
Production	Industrial espionage Disclosure of goods flows Disclosure of business relationships
Logistics	Industrial espionage Disclosure of goods flows Disclosure of business relationships
Intelligent home	Profiling of personal property, consumer behaviour, lifestyle, possibly also of social contacts and activities Indirect disclosure of sensitive data (e. g. illness among the population related to ONS queries about medication)

3.1.3 Relevance of ONS business models

This study mainly examines security issues raised by the ONS's current organisation and technical architecture. However, the business models on which the technical implementations are based will also have a major bearing on the correct operation and security of the ONS and on other components of the EPCglobal architecture. With this in mind, the following organisational issues are also relevant:

- Rules for delegating and allocating EPCs
- Procedures and juridical authorities for last resort dispute resolution
- Delegation of registry services
- Operational security of the registry and validation
- Requirements for and accreditation of registry service providers

3.2 Multipolar ONS

This section covers modifications to the current ONS architecture (multipolar ONS, MONS), which enable distributed control of the ONS root between various independent users, thus resolving the problem of unilateral control of the root.[14]

3.2.1 Technology and organisation

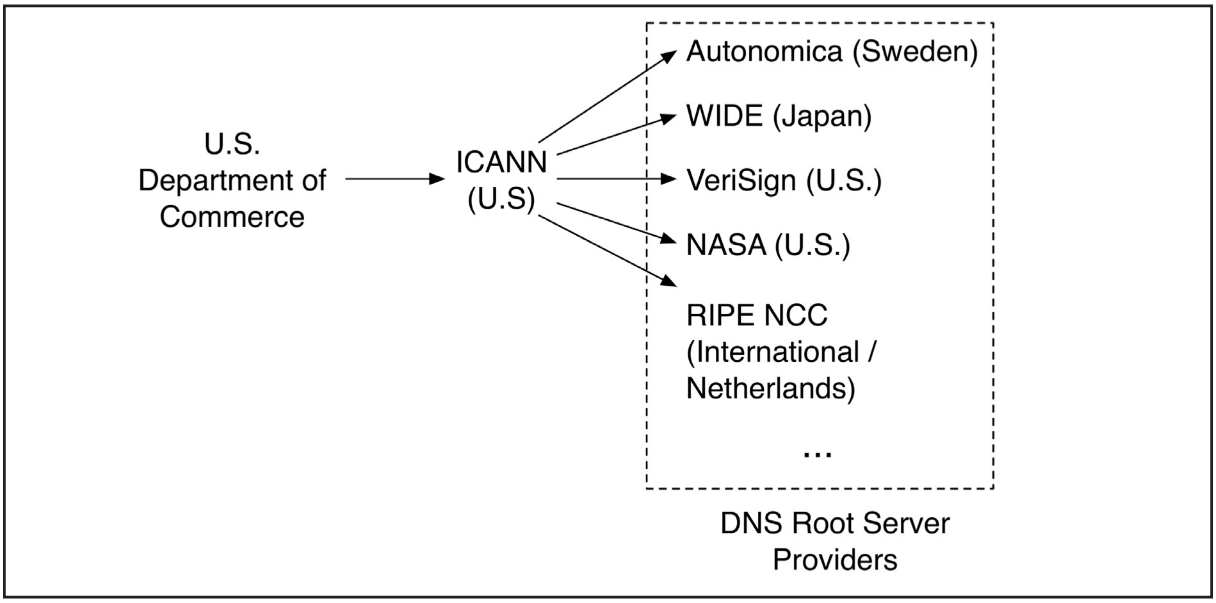
Before proposing modifications designed to solve the problem of unipolarity in the existing ONS architecture, we should consider the following question: How serious is the problem of unipolarity in the original DNS?

In technical terms, the DNS is a hierarchy of DNS nameservers, in which each server is responsible for resolving the host names (e. g. of websites) belonging to its domain into IP addresses or assigning the names to another DNS nameserver when a delegation takes place.[15] The DNS nameservers that have authority for top-level domains (TLDs, e.g. .eu, .com) are operated by special registry bodies – organisations that are responsible for the administration and technical operation of the TLDs. The root nameservers are operated by state authorities, commercial and non-profit organisations. The root zone is managed by the non-profit US company „Internet Corporation for Assigned Names and Numbers“ (ICANN). ICANN was officially contracted for this by the U.S. Department of Commerce, thus implying a legal control of the US ministry over the root namespace.

At present, the root zone is served by only 13 logical root nameservers. Technical limitations prevent this number from being increased easily. However, many of these servers have been mirrored in numerous other regions and can be accessed via Anycast[16]. As a result, most of the physical root nameservers are now situated outside the US.

However, the Internet community has constantly criticised this concentration of legal control over the DNS root namespace within the hands of a single government body. In theory, the body is empowered to make changes to the root zone file.

Figure 9: Power structure within the DNS


U.S. Department of Commerce
ICANN (U.S)
Autonomica (Sweden)
WIDE (Japan)
VeriSign (U.S.)
NASA (U.S.)
RIPE NCC (International / Netherlands)
...
DNS Root Server Providers

[14] See [EFG08].

[15] See [LA06].

[16] Anycast is a protocol for „one-to-many“ correspondence between an IP address and several, physically distributed servers: this means that the most suitable server (usually the nearest) is selected for each query (see RFC 3258).

However, due to the de facto dispersal and mirroring of the root zone, any changes would have to be propagated to all other root nameservers, many of which are outside the jurisdiction of the US body controlling the root zone. If this body decided to abuse its power and introduce changes to the root zone to serve its own interests, some root nameservers could refuse to carry out the changes to their own root zone files. This could ultimately result in uncontrolled and permanent fragmentation of the central naming system of the Internet. It could also undermine the basic principles of the Internet, thus increasing business risks globally.

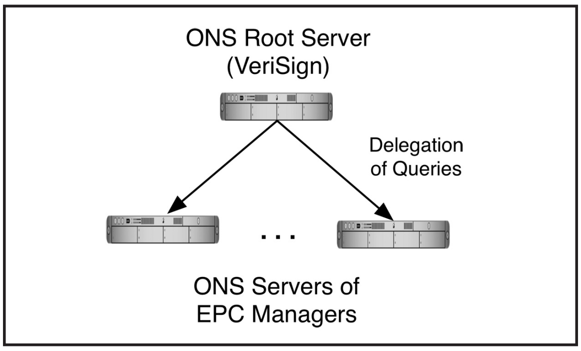
These implications and the fact that so far no such changes have been made, allow us to assume that the Internet is not in fact so dependent on the body managing the root namespace, and that it is highly unlikely that this particular body will independently make any changes that would impede fair, global Internet access. It is therefore unrealistic to imagine that a country might initiate a root blocking attack on the DNS and run the unpredictable risks such an attack would entail. In contrast, the ONS might well be subject to that type of attack, particularly in the event of military conflicts.

The following sections outline a proposal for modifying the current ONS architecture. The aim is to distribute control of the ONS root among several, independent participants and thus eliminate the problem of unilateral control of the root.

3.2.1.1 Replicated MONS

One of the main reasons why DNS was selected for implementing the naming service for the EPCglobal network, was to facilitate the introduction of the ONS on a global scale. The DNS is considered by many experts to be a mature and proven architecture in principle. Choosing the DNS allows the ONS to be deployed using existing DNS software while relying on best practice acquired through years of DNS use. A system administrator with experience working with DNS can therefore relatively easily take over the deployment of a local ONS nameserver with freely available software. If we want to modify the existing ONS architecture, it makes sense to retain compatibility with the DNS protocol.

Figure 10: Current ONS hierarchy



As originally planned, the ONS root was to be implemented across six globally distributed server constellations, all operated by VeriSign (Figure 10). This is in strong contrast to the DNS architecture, in which the root nameservers are operated by a number of independent entities. One possible way of avoiding the unipolarity of the ONS is to reproduce the ONS root on a large number of servers operated by independent entities synchronising the instances of the root zone file with a master copy published by EPCglobal. To limit the number of incoming queries, each root nameserver could be configured to cover a particular area within the IP topology and only respond to queries originating from there.

These mirrored ONS root nameservers could offer their services in parallel to the global ONS root operated by VeriSign.[17] The resolving ONS servers of organizations and Internet Service Providers (ISP) should be configured on the one hand with the domain name or IP address of the global ONS root (onsepc.com), or, more efficiently, the server responsible for SGTIN (sgtin.id.onsepc.com), on the other hand also with the corresponding replicated ONS server (e.g. sgtin.id.onsepc-replication.eu), potentially avoiding Anycast constructions like those used as later add-ons for DNS.

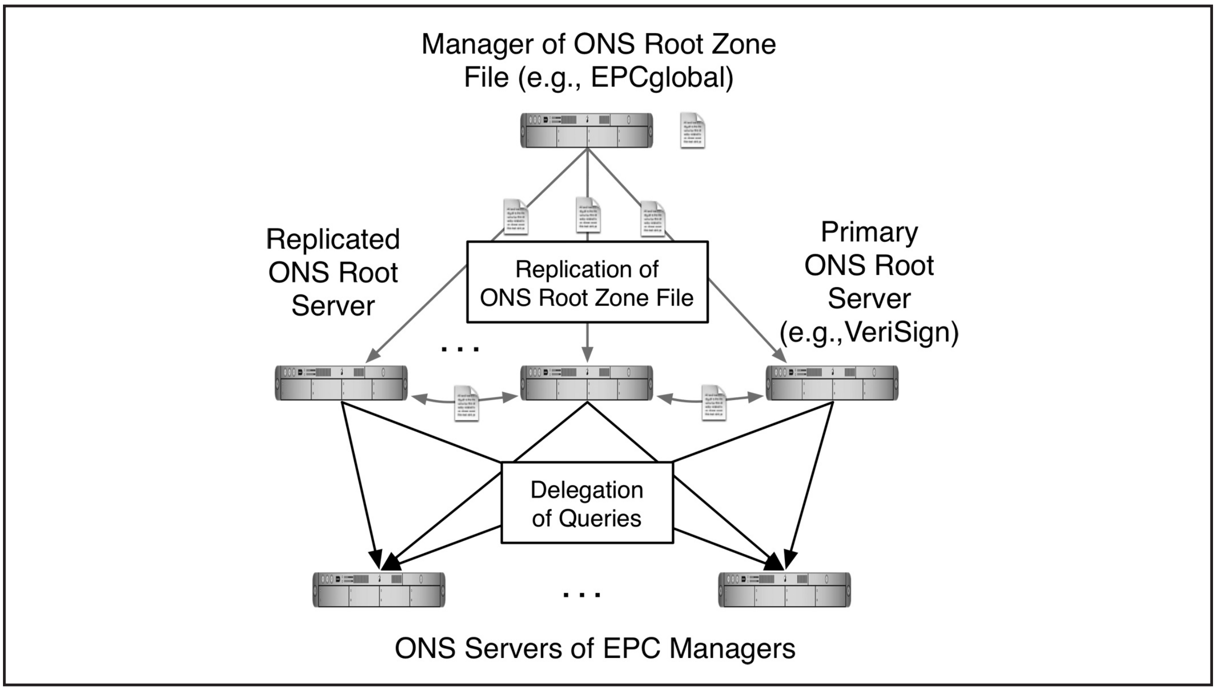
To evaluate the feasibility of this approach and the amount of data that has to be replicated, we approximately calculate the size of the ONS root zone file by estimating the number of RRs stored there, which define mappings between Company Prefixes and domain names of the corresponding ONS nameservers.

Today there are already over a million registered company prefixes.[18] We assume that most of these will have corresponding EPCIS at some stage in the future. The ONS root zone file is a plain text file consisting of a number of NS RRs (nameserver RRs). Let us take the example of an EPC number 400453.1734.108265, which can be resolved into one of two ONS nameservers to delegate the query there:

1737.400453.sgtin.onsepc-com IN NS ons1.company.com
1737.400453.sgtin.onsepc.com IN NS ons2.company.com

IN stands for „Internet“ and „NS“ indicates that the record defines a nameserver that is authoritative for the domain. The number of nameservers responsible for the same zone must not exceed thirteen; the DNS specification recommends using at least two.

Figure 11: Replication of ONS root


Manager of ONS Root Zone File (e.g., EPCglobal)
Replicated ONS Root Server
Replication of ONS Root Zone File
Primary ONS Root Server (e.g.,VeriSign)
. . .
Delegation of Queries
. . .
ONS Servers of EPC Managers

[17] Up until recently, there was a similar alternative for the DNS root: The independent Open Root Server Network, run by Internet volunteers, was forced to shut down at the end of 2008 (http://european.ch.orsn.net/), see also the German website Heise Netze (23.10.2008): http://www.heise.de/netze/Alternative-DNS-Root-Server-vor-der-Abschaltung--/news/meldung/117863.

[18] See http://www.gs1.org/productssolutions/barcodes/implementation/ (10/2008).

In practice, the number varies between two and five. Assuming the average number of ONS nameservers per company (N) is four, the average length of an NS record (L) is 60 characters (where one character requires one byte). The number of registered company prefixes (P) is in the region of one million, for the reasons described above. We can thus use N x L x P to provide a rough estimate of the size of the ONS root zone file containing the RRs for all currently registered EAN.UCC company prefixes: this estimate would amount to just over 200 MB.

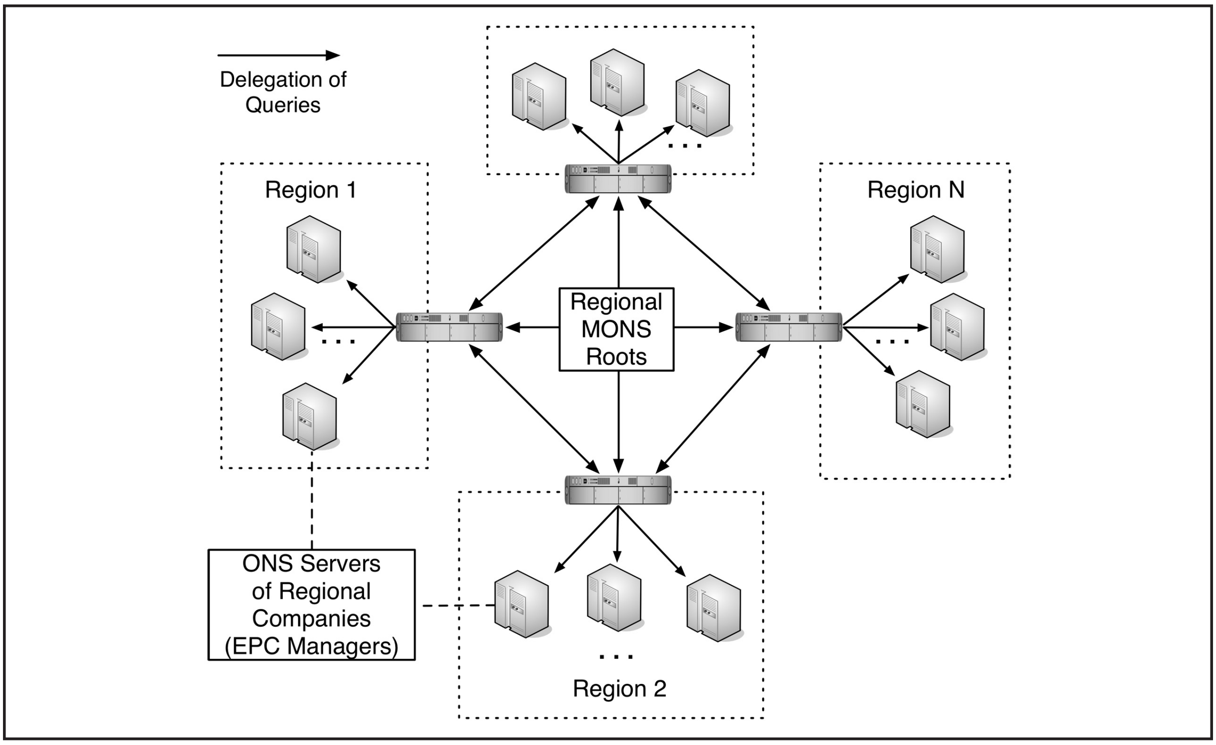
Compression can be used to reduce a text file to 10 or 20% of its original size. The distribution and regular renewal of the root zone file should not therefore present any technical difficulties. The master root zone file can be shared between the ONS roots with a simple file transfer or a specially secured peer-to-peer filesharing protocol. Figure 11 shows the architecture used. This is referred to in the following section as the replicated MONS.

Public availability of the ONS root file is a key prerequisite for Replicated MONS. As soon as the root zone file is published and regularly updated, the mirrored roots can be deployed independently of each other. If those new roots are configured to cover only certain areas, locations beyond their bounds will still be able to use VeriSign's nameservers, remaining vulnerable to the Blocking Attack.

3.2.1.2 Regional MONS

The architecture described in the previous section offers a solution that gives any entity the technical means to maintain a copy of the ONS root nameserver, thus enhancing the availability of the ONS. It could also lead to an unstructured patchwork of areas with greatly varying ONS root redundancy (in global terms).

Figure 12: Regional MONS



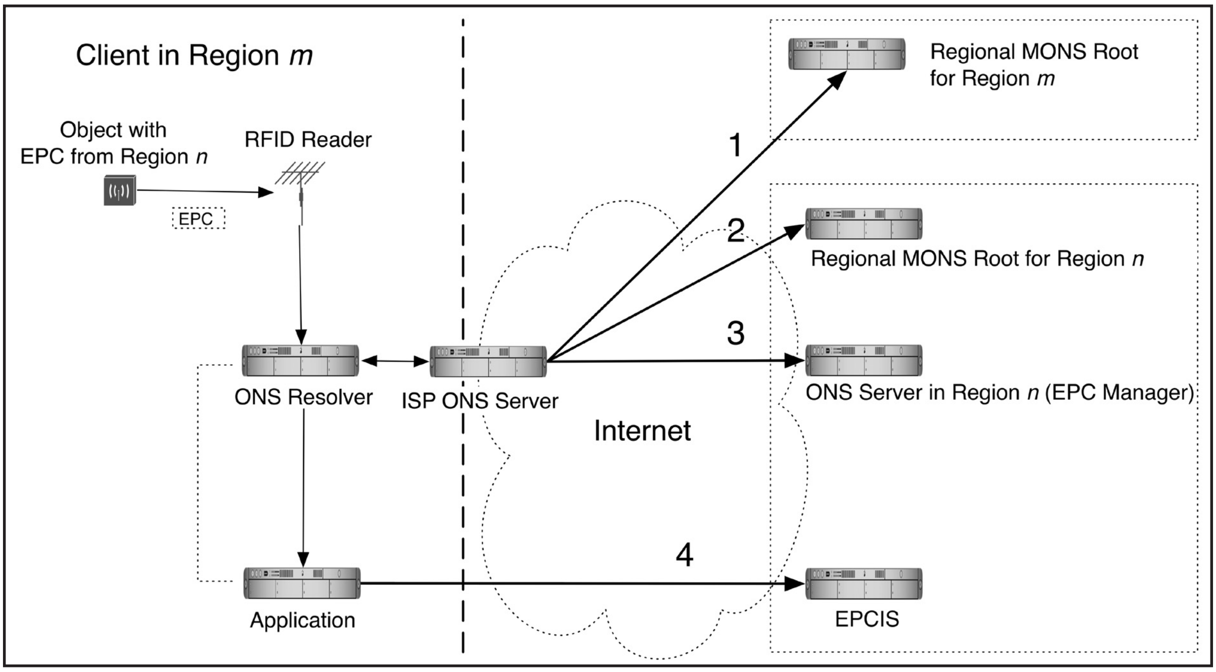
The high load on the root nameservers will be mainly caused by the size and frequent updates of the root zone file. Compared to the root zone file of the DNS, which contains RRs on about 1500 TLD nameservers and currently has a size of about 70 kilobytes, the ONS root zone file will contain RRs for all EPC Managers' ONS nameservers registered at EPCglobal. Since the use of RFID and EPC is expected to become ubiquitous, the number of EPC managers is likely to grow quickly, resulting in millions of RRs. Furthermore, due to a higher volatility of RRs of the ONS root, their TTL parameters can be assigned lower values compared to the RRs of the DNS root. As a result, the ONS RRs will be cached for shorter periods of time and a larger number of queries will reach the ONS root nameservers.

In this section, we look at another, more radical alteration of the existing ONS architecture, which will enable a reduction in the size of the root zone file and the frequency of its updates by splitting it between several *regional root servers*.

The zone file of each regional root nameserver contains RRs corresponding to the EPC Managers belonging to a region for which the nameserver is authoritative. Membership of a region can be determined by means of the address under which the company is registered, the regional GS1 organisation that issued the „Company Prefix", or by other properties.

Figure 12 shows this architecture. Figure 13 shows the associated process of EPC resolution. In case the resolving nameserver and the EPC Manager (that corresponds to the EPC being resolved) belong to the same region (n=m), the second step should be skipped. The resolution process is nearly identical to the process used in the standard ONS in Figure 2. The regional root nameserver directs the query to the nameserver of the EPC manager, which returns the addresses of the EPCIS. Otherwise, if n≠m, the query is redirected to the regional root nameserver that is authoritative for region n (step 2). This root nameserver then sends the query to the EPC manager's nameserver. We refer to this architecture as *Regional MONS*.

Figure 13: Query process for Regional MONS


Client in Region *m*
Object with EPC from Region *n*
RFID Reader
EPC
ONS Resolver
ISP ONS Server
Application
Internet
1
2
3
4
Regional MONS Root for Region *m*
Regional MONS Root for Region *n*
ONS Server in Region *n* (EPC Manager)
EPCIS

This differs from the ONS resolution process in that delegation of a request from a regional ONS nameserver to another (step 2) involves an additional resolution step. Consequently, this requires an extension of the EPC scheme and the introduction of a new prefix that will be resolved in this step. One obvious option would be to have a regional prefix that points to the country or region of the product's origin, comparable to the standards for composing an EPC. Introducing this type of regional prefix would require a change to the EPC coding standard, possibly resulting in a costly and time-consuming process.

However, the EPC encoding schemes already include sufficient information to enable unambiguous association of an EPC with a region. The first three digits of the EAN.UCC company prefix identify the GS1 regional office that issued the EAN.UCC to the company, e. g. the codes 400-440 are reserved for Germany. An alternative to introducing new regional prefixes would therefore be to use these numbers to associate the EPCs with the relevant regions.

The resolver still views the Regional MONS as a hierarchy: The MONS root of its region is perceived as a root of the entire hierarchy. We refer to this type of structure as the relative hierarchy. A regional nameserver that is authoritative for the region where the resolution occurs is called a relative root. This allows the Regional MONS to be implemented within the DNS framework, in line with the approach described in the ONS specification.

In the following section, we assume that the regional prefix is defined by the first three digits of the company prefix. Accessing the EPCIS that can deliver data about a particular EPC requires first that the EPC be translated into a DNS-compatible name, as with the ONS. However, the first three digits of the EPC Manager must now be explicitly separated by dots and positioned to the right of the rest of the inverted EPC name (e. g. 1734.453.400.sgtin.id.onsepc.com).

Let us assume that the DNS name of the regional nameserver that is authoritative for the zone 400.sgtin.id.onsepc. com is ns1.mons.eu. An ONS client that is physically situated in the same region is configured so that it sends all ONS queries to ns1. mons.eu (step 1 in Figure 13), which it views as a relative root of the Regional MONS. Accordingly a resolver that belongs to another region would be configured with the address of another regional root, viewed therefore as a relative root.

In this example, we deliberately chose the domain name of the regional root to have the TLD (.eu) corresponding to the region of its authority. This avoids the dependency on entities administering regional nameservers and excludes the possibility of a Blocking Attack from their side.

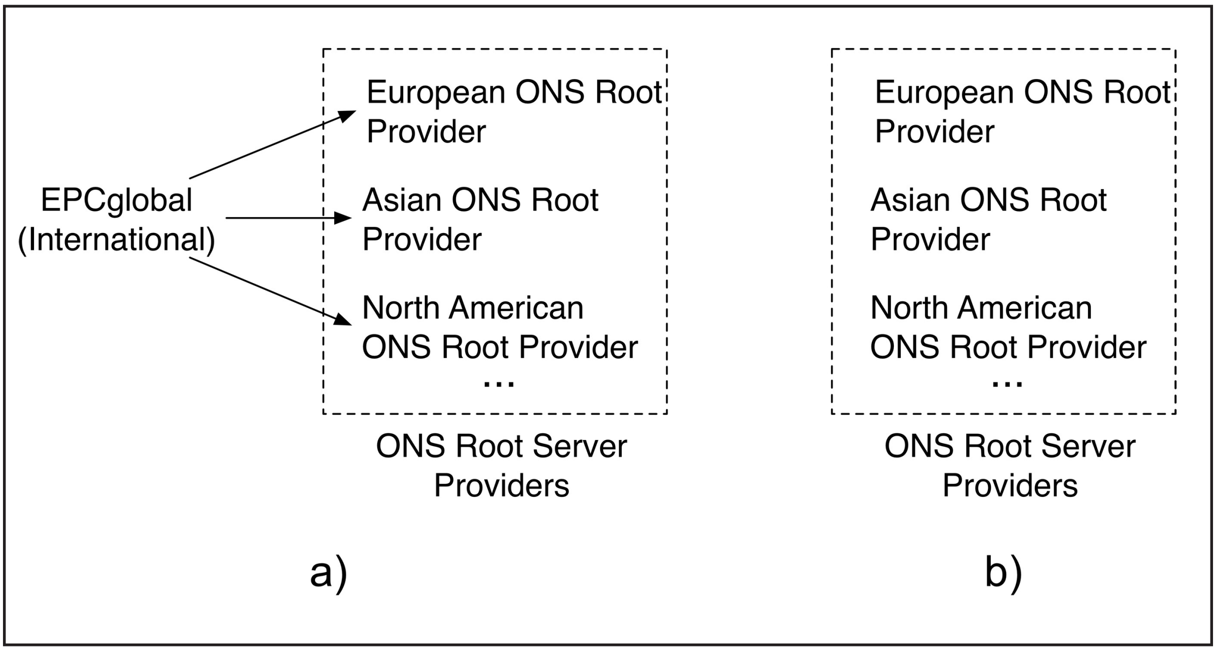
Since certain nameservers are unambiguously assigned to regions, the Regional MONS naturally shifts the highest load to those nameservers that have authority for economically developed or industrial countries: The regional prefixes for these regions appear in most EPCs and most queries are sent from these regions. In addition, regions whose export values are too low or that are not interested in maintaining their own regional MONS root, can delegate this responsibility to third parties, as is sometimes done with the TLDs in the DNS. If their situation changes, these countries can recover their reserved share of the system by making small changes to the table of regional MONS roots (MONS root zone file).

3.2.1.3 Power structure

Figure 14 illustrates possible power structures for the MONS architectures described in this section. Each replicated or regional ONS root server is maintained by a corresponding regional company.

In the case of the replicated MONS, a central instance is still required (e. g. through EPCglobal in this example). The Regional MONS does not require a central instance for coordination because each regional root is deployed independently from the others and the role of EPCglobal would be limited to simple administrative tasks.

Figure 14: Example of possible power structure, a) Replicated MONS b) Regional MONS


EPCglobal
(International)
European ONS Root Provider
Asian ONS Root Provider
North American ONS Root Provider
...
ONS Root Server Providers
a)
European ONS Root Provider
Asian ONS Root Provider
North American ONS Root Provider
...
ONS Root Server Providers
b)

3.2.1.4 Economic aspects

The incentive problem mentioned in section 3.1.1.3 also applies to the MONS architecture described here. However, the decentralisation of MONS could result in a more flexible system of payments, as most of the costs incurred through maintenance of the ONS root servers are borne by the relevant regional organisations (e. g. regional GS1 divisions). At present, the charges for companies with a turnover of up to 250 million USD is fixed by the local GS1 divisions, while the charges for companies with a turnover of over 250 million USD is fixed by the EPCglobal price list.

3.2.2 Security

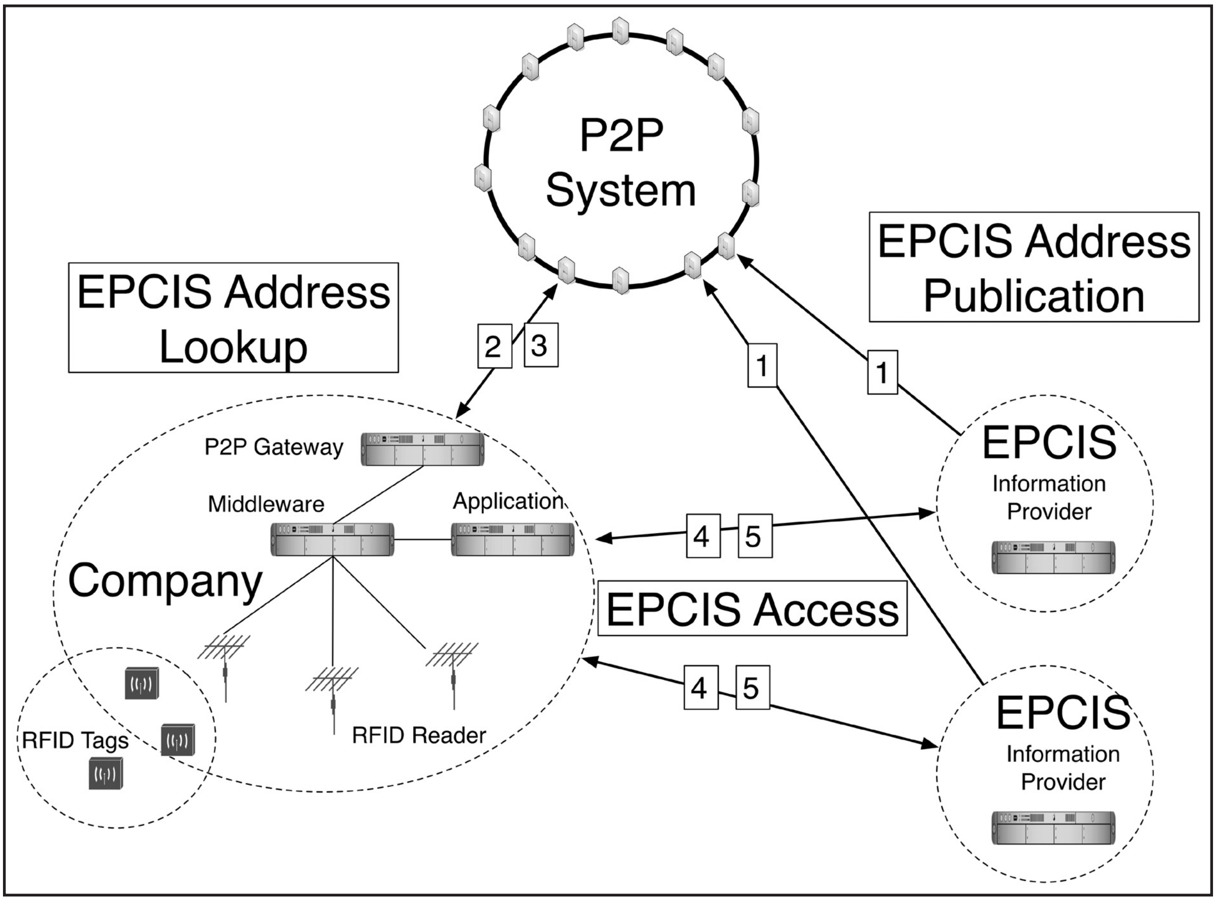
MONS was not designed to provide a solution for the general problems of integrity, availability and confidentiality in the ONS. It is a DNS-based architecture designed with the main objective of solving the problem of unipolarity. However, the integrity problems can be solved with the additional deployment of DNSSEC (see section 3.4).

3.3 Peer-to-Peer ONS

Alternative architectures to the ONS may be based on peer-to-peer architectures (P2P), which offer much greater flexibility in the handling of client and server roles than is possible in conventional distributed systems.

Both roles can be executed simultaneously by all participating nodes in a network. Peer-to-peer networks are therefore significantly less centralised and usually consist of equal partners, also known as nodes. The EPCIS addresses can also be saved as documents in these P2P systems and called up again at a later stage (see Figure 15).

Figure 15: Example of a P2P ONS architecture



3.3.1 Technology and organisation

A distinction is often made between structured and unstructured P2P systems. If unstructured, the P2P system is allowed to grow largely unchecked and there is no assignment of data to specific nodes. The advantage of these systems is that they can handle a high fluctuation in participating nodes; the disadvantage is that, with a high number of participants, search queries become very inefficient because for the most part they must be flooded non-directionally through the entire network. Hybrid P2P systems, as they are known, can help by making searches easier with centralised index servers. However, these centralised index servers unfortunately also provide easy targets for attacks on the system.

3.3.1.1 Advantages and challenges of peer-to-peer systems

Structured P2P systems based on distributed hash tables (DHT) represent a very promising direction for research, particularly for infrastructure networks.[19] Even with large numbers of participants, DHT systems are generally highly scalable and robust in the event of failures and targeted attacks. They avoid dedicated nodes (e.g. hierarchy roots such as the ONS root) and thus a single point of failure and systematically distribute memory load and responsibility between participants. This distribution is facilitated by forming a topological „overlay“ structure in which the nodes and data addresses can be systematically inserted and deleted again without requiring a central instance or global modification to the network. A DHT provides simple memory and search functionality based on a correspondence between search keys, data and the actual computers that form the network.

However, using P2P systems also gives rise to new challenges. The integrity of the saved documents is not necessarily guaranteed when simply switching over to a P2P architecture for ONS, even if the participating nodes are infrastructure computers run by companies and not ordinary desktop PCs. In general, however, the confidentiality and anonymity of queries could be enhanced because a central initial query instance such as the ONS root or several MONS roots would not be used. Other attack vectors on the confidentiality of queries such as the reading of IP packets would still be relatively easy to execute. Generally, therefore, P2P architectures must provide additional protective mechanisms if they are to offer benefits other than their greater robustness and superb scalability compared to the traditional ONS. The following section illustrates an example of a P2P ONS that provides additional security.

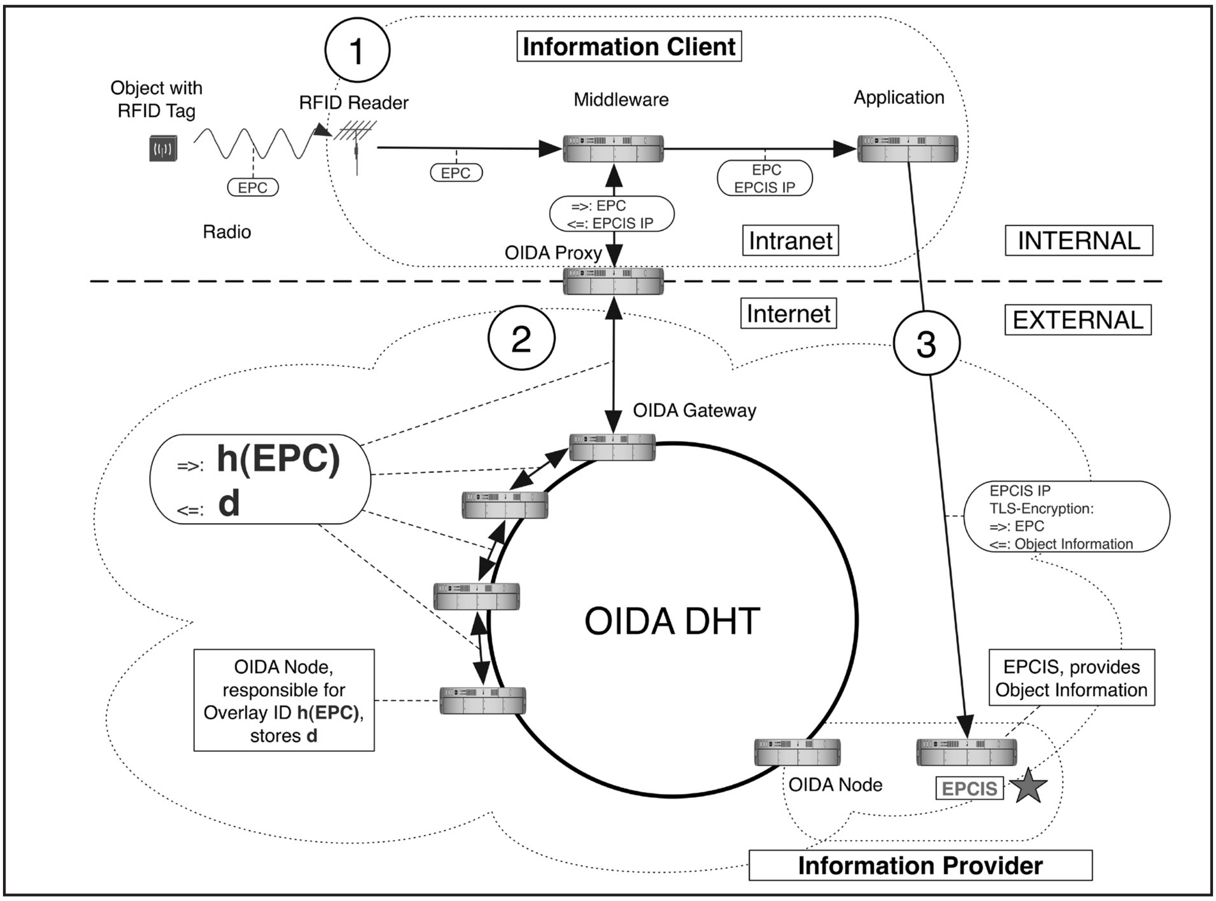
3.3.1.2 Object Information Distribution Architecture (OIDA)

This section describes a DHT-based P2P ONS known as Object Information Distribution Architecture (OIDA).[20] OIDA is intended to act as a global infrastructure network for ONS and incorporates a number of important ideas. Each company interested in participating provides dedicated OIDA nodes, i.e. computers which, like DNS or ONS servers, execute just one task for performance and security reasons. These nodes form an overlay network based on a fixed distributed hash table (DHT), in which a cryptographic hash function maps EPCs and physical nodes in a topology of overlay identifiers, whose particular properties depend on the specific DHT selected. This pseudo-random assignment of data and storage nodes ensures more even load distribution than with the ONS, where, for example, the ONS root is expected to bear a particularly heavy load. It also reduces the risk of targeted attacks being mounted on the data of specific companies.

[19] See [BKK03]

[20] See [FG07]

Figure 16: Query process in OIDA

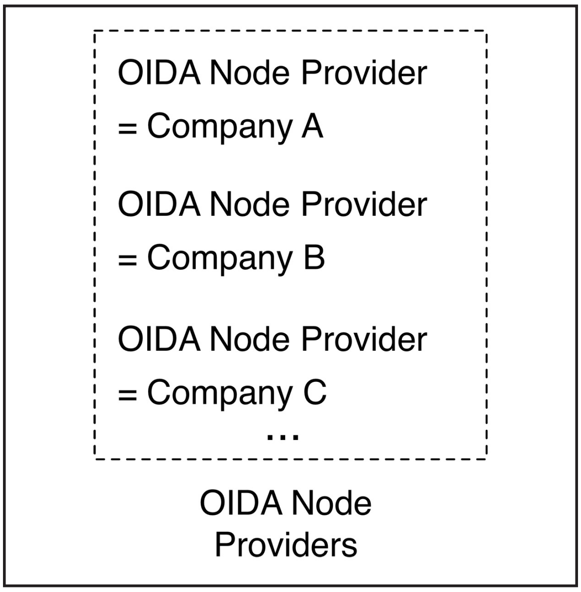


The DHT is responsible for routing queries to the nodes where the required information is stored (Figure 16). The DHT software is also responsible for the decentralised management of protocols, which govern the addition and removal of nodes and the repair of the DHT in the event of spontaneous node failures.

3.3.1.3 Power structure

Figure 17 shows potential power structures in the OIDA. Each OIDA node is operated by one company that is interested in making its product information addressable at a global level. There are no specific intermediaries (e.g. ONS root operators) in the architecture because OIDA nodes assign the queries directly and correctly among themselves according to the addresses of suitable EPCIS.

Figure 17: Power structure in OIDA



3.3.1.4 Economic aspects

The cost distribution issue referred to in section 3.1.1.3 is also relevant to the OIDA. However, as this architecture does not require an infrastructure that is operated by third parties, such as the root server in the ONS, subscription charges could be reduced significantly or even completely eliminated.

On the other hand, an architecture that is distributed in this way can lead to new types of incentive problems. Since an OIDA node is highly unlikely to have saved any of its own address data but rather the data of other companies, there are no direct incentives to participate appropriately in the OIDA, i.e. to operate the nodes appropriately and correctly, guarantee their availability, ensure updates, hardware upgrades and sufficient connectivity to keep response times short.

This affects both the OIDA and other similar P2P architectures in which the information provider's data are stored separately. Most existing P2P networks are not considered part of a critical infrastructure but are operated by volunteers and their areas of application do not incur any specific expenditure or maintenance costs.

In the case of a P2P-based naming service, additional measures may be necessary to check that the hardware and overlay network are functioning correctly and to guarantee that such a system is capable of performing a naming service for thousands of companies. Applying proper contracts and monitoring of availability would be the appropriate options. Even with P2P ONS, a central instance may therefore be necessary to ensure that participants take part appropriately.

3.3.2 Security

The documents containing EPCIS addresses are stored on the OIDA nodes in encrypted form and in conjunction with the information provider's digital signature, which allows the end user to monitor the integrity and authenticity of the information. The documents should include the IP addresses of the EPCIS and not their DNS names so that they are independent of the authenticity of the global DNS.

For scalable implementation of the signatures for the data, a central certification body, e.g. run by EPCglobal, a hierarchical trust infrastructure such as DNSSEC or a decentralised „Web of Trust“ such as PGP, which is used for email, could be deployed. This infrastructure must be assessed in turn for security, economic and political implications and further developed if necessary (see also Section 3.4 on DNSSEC).

The following table shows the main security features of OIDA and their effects.

Table 6: OIDA security features

Feature	Effect	Positive effect on:
DHT architecture (peer-to-peer)	No root, no designated nodes. No single point of failure/control/attack	Availability, multipolarity
	Decoupling of information provider and information storage location. „Random“ selection of documents on each OIDA node ► Less motivation for systematic log file analysis by OIDA nodes	Confidentiality of client query (with regard to operator and ISP of the OIDA node)
Replication convention	Almost any number of address document copies	Availability, multipolarity
Digital signatures on documents	Authenticity of documents can be checked by client even if they come from an uncertain source	Integrity of the documents (against modification by third parties)
Optional: PKI for securing OIDA nodes (PKI node)	Increased integrity against external attacks aimed at manipulating the DHT (publication phase, routing, messages about the non-existence of documents)	Integrity of the DHT, availability of documents
Cryptographic hash function of the DHT	EPC is not transferred in plain text	Confidentiality of the client query (with regard to all ISPs, Internet Backbone, OIDA nodes)
Encryption of documents	The response is not transferred in plain text. ► Query cannot be inferred indirectly	Confidentiality of the document (with regard to third parties), confidentiality of the query (with regard to third parties and information) providers)
Recursive routing in the DHT	The identity of the client remains hidden during the communication process within the DHT especially for the relevant OIDA node	Anonymity of the client (with regard to the provider, OIDA nodes and many third parties – but not with regard to the client’s ISP or the OIDA gateway that it uses)
SSL/TLS between client (OIDA proxy) and OIDA gateway	Encryption and authentication of the connection to the OIDA gateways	Confidentiality and integrity (with regard to the client's ISP, Internet Backbone, but not with regard to the OIDA gateway)

In short, it has been established that OIDA could decouple the resolution of EPCs into EPCIS addresses completely from the traditional DNS infrastructure and its protocols. This would also avoid overloading of the infrastructure by new applications based on the Internet of Things. At the same time, OIDA provides greater confidentiality and anonymity plus simple replication mechanisms to increase data availability and, assuming global participation, avoids unipolar power structures. Even in P2P infrastructure networks such as OIDA, a central instance, e.g. an independent international committee or consortium, can be important for organisational tasks, security infrastructures, availability monitoring and software updates.

All naming service architectures (e.g. ONS, MONS, OIDA) must take into consideration the security and multipolarity provided by the accompanying technical security infrastructures. An important example of such an infrastructure is DNSSEC, which is described in the next section.

3.4 DNSSEC – Security function and new challenges

DNSSEC (DNS Security Extensions) is an important set of mechanisms for ensuring authenticity and integrity for the DNS.[21] DNSSEC can also play an important role in guaranteeing the integrity and authenticity of ONS and DNS-based variants such as MONS, but the technology involves new challenges in these areas.

First, DNSSEC offers mutual authentication of DNS servers on the basis of shared secrets. However, this procedure offers limited scalability. A more important technology that is integrated in DNSSEC ensures authenticity and integrity of the actual DNS data. This uses public keys (public-key cryptography) and signatures that are verified via chains of trusted instances.

At present, DNSSEC is rarely used in practice. Some of the reasons for this may be linked to the difficulty of creating trust relationships outside small „islands of trust“. Guaranteeing data integrity in ONS by means of DNSSEC would require ubiquitous use. For scalable management of these challenges, it is possible to create a tree of trust relationships parallel to the DNS name hierarchy: in theory you then only need to know a few public keys (e. g. the key of the DNS root) to verify the DNS data by following the delegation path and checking the trust chain for gaps.

Even if DNSSEC could enable encryption of DNS information (an option so far explicitly excluded by the corresponding standards), the Company Identifier (EPC Manager) of a queried EPC could at least be identified though Internet traffic analysis. This identification would simply require observation of the IP addresses to which the ONS queries and subsequent EPCIS communication are sent. Furthermore, DNSSEC does not protect the availability of the service in any way.

[21] See [RFC4003]

A recent topic of political discussion is the question of which entity should control the keys for the DNS root zone. They are currently under the control of the US.[22] If the ONS is restructured to offer multipolarity, the change should occur at the same time as the related DNSSEC trust infrastructure is set up, if this is to be used with ONS. In this case, it should be noted that many DNS names that may appear in the URL entries of the ONS-RR (which can include arbitrary DNS names) must be connected authentically by means of DNSSEC with their IP addresses. DNSSEC for ONS must therefore not be limited solely to securing the ONS subtree of the DNS (onsepc.com and subdomains), as this would create gaps in integrity assurance.

3.5 The role of IPv6

IPv4 is the currently established Internet protocol used for correct addressing and routing of data pakkages in the Internet. IP addresses are essential for communication partners wishing to connect to the Internet. However, IP addresses for IPv4 will become scarce in the next few years.

As early as in 1995, the Internet Engineering Task Force (IETF) decided on a successor to the Internet protocol IP: IPv6.[23] Until now, the older version IPv4 has remained dominant. However, widespread use of IPv6 may soon become necessary, particularly among Asian countries with scarce IPv4 address space and for mobile devices.

IPv6 offers many advantages compare to the previous protocol. Since IPv6 uses 128-bit addresses, the supply of addresses is far greater than offered by IPv4 and its 32-bit addresses. This allows a generous allocation of subnetworks, which also simplifies the routing tables used throughout the Internet. The routers benefit from a simplified IP header, shifting of options to „extension headers“ and avoidance of fragmentation. Part of the security protocols for IPv6 have been backported for IPv4 in the form of IPSEC (IP Security). IPSEC is a mandatory component for IPv6.

From the very outset, mobility of IP-networked devices was a vital design component for IPv6. Even at that stage, the protocol was expected to play a major role in the Internet. In addition to autoconfiguration (automatic generation of an IP address from a prefix specified by routers), the Mobile IPv6 protocol is a key technology that particularly supports mobile devices, which have frequently varying locations and network connections.[24]

[22] See e. g. the collected sources at heise.de:
http://www.heise.de/security/VeriSign-will-DNSSEC-Schluessel-ein-bisschen-teilen--/news/meldung/116903 and
http://www.heise.de/newsticker/IGF-Schlagabtausch-zum-Einfluss-der-Regierungen-im-DNS--/meldung/120035.

[23] See [RFC2460], [Los04].

[24] See [Sol04].

For a future, genuine Internet of Things beyond RFID, i.e. with full IP implementation on chips belonging to objects, convergence towards IPv6 could occur on the network layer – irrespective of the particular physical communication medium used (e. g. RFID, WLAN, Bluetooth, WiMax or UMTS). Planned migration processes and tunnelling methods used to transport IPv6 packages to IPv4 packets, for example, could enable a connection to established IPv4 infrastructure and facilitate the integration of Smart Objects in existing networks.

In this type of scenario, a naming service like ONS would be used not just for looking up EPCIS, but also for finding the IP addresses of actual objects by means of their ONS name: this would allow the objects to be contacted directly from the remote Internet. Sustaining a scenario with billions of IPv6-networked objects could create even bigger challenges for the naming service infrastructure in terms of scalability and query load than those faced by the implementation of the ONS purely for RFID tags or required for DNS use in today's Internet.

4. Interview findings

As part of this study, interviews were held with experts from industry and the scientific field to obtain their views on the current ONS discussion. The following companies generously gave of their time for interviews: CBR (fashion clothing), Deutsche Post World Net (logistics), Gerry Weber (fashion clothing), IBM Deutschland (information technology and systems integration), Kaufhof (retail), Lufthansa Technik Logistik (aviation, logistics), METRO Group Information Technology (IT service provider for trade and retail), Psipenta (software and systems integration), Robert Bosch (medical technology), Seeburger (software and systems integration), and Volkswagen (automotive industry). In addition, interviews were held with the associations AIM-D (identification systems) and VDMA (mechanical engineering) and with the Bremer Institute for Production and Logistics at the University of Bremen (BIBA).

Many of the companies contacted were either entirely unfamiliar or only vaguely familiar with the topic of the ONS. One large German car manufacturer and a large telecommunications provider responded that they did not want to comment publicly on the subject. Several owners of small and medium-sized companies expressed their willingness to take part in an interview, although they did not have a detailed knowledge of the subject matter. Among the interviewees, the technology users and subscribers responded positively because they had generally already carried out RFID projects and consistently had more in-depth knowledge of RFID technology and of the debate currently surrounding ONS.

Most of the interviewees requested that the views expressed be treated as confidential. Therefore most of the statements that follow cannot generally be attributed to individual interviewees.

The interviewees were presented with the problematic topic in advance of the discussions (see Chapter 2). They understood the topic and considered its focus on five problematic aspects (unipolarity, ONS-internal power structures, integrity, availability, confidentiality and anonymity) as mainly comprehensive and constructive. However, one participant commented that the EPCglobal Network and the ONS could not be equated with the Internet of Things - the EPCglobal Network and the ONS are only the early elements of an infrastructure for the Internet of Things. Most of the interviews also discussed the current relevance of the ONS.

General relevance of the ONS

Among the interviewees, the users were unanimous in considering the ONS to be only of minor relevance to their business or sector. Reasons given were the fact that consumer products equipped with RFID tags are not yet in widespread use; that in some cases, RFID is already integrated in existing EDI systems and that other identification systems are in competition with RFID. Views differed as to whether or when the ONS or the EPCglobal network would become a topic of strategic relevance for the users. They ranged from an inability to foresee the added value of the ONS to the belief that ONS or the EPCglobal network and its services could replace outdated EDI systems.

In rating the relevance of the ONS or the EPCglobal network, the technology providers among the solution providers consistently referred to their customers' decisions; their own strategic interests were not mentioned.

Unipolarity and power structures

The risk of technical outage associated with a centralised ONS services (if mentioned at all by the interviewees) was considered to be both minimal and manageable. Views of the political risks varied widely. Some of the users considered the ONS service to be irrelevant to using RFID or EPCglobal within their own sector, and thus did not associate any risks with the deployment model. Other participants cited possible risks linked to a private sector ONS operator within a national jurisdiction, such as arbitrary restrictions imposed on services or system shutdowns. The DNS service for the Internet and the GPS navigation service were mentioned as negative examples. One participant stated that Russia and the Middle East might be reluctant to accept a US-dominated EPCglobal system.

Other interviewees dismissed the risk of a US-based operator possibly abusing the ONS service. This was deemed particularly unlikely because the EPCglobal Network would only be an extension to established and trusted IT infrastructures for data communication between companies. Direct 1-to-1 communication with known partners (where the ONS service is unnecessary) would remain the most common procedure for the foreseeable future.

Several interviewees strongly believed that EPCglobal should be developed by an industry body focusing on trade and the consumer goods sector, rather than by a neutral standardisation organisation. Charges for using the EPCglobal network were considered by some to be a partial barrier to use, especially for SMEs.[25]

Integrity, availability, confidentiality and anonymity

Most of the interviewees considered a differentiated concept of authorisation and access to be an essential requirement for a practical EPCglobal network for their business or sector. The potential risk of profile generation for products and business was raised several times. In general, technical obstacles to implementing an appropriate security infrastructure are not a concern. However, many companies stressed the importance of having general guidelines for implementing and operating such a security system and compliance with these guidelines: Companies in the network must be able to trust the security measures of all other partners. One interviewee cited the current *Technical guidelines for secure RFID implementation* compiled by the German Federal Office for Information Technology Security (BSI). There is a high level of awareness regarding the protection of personal data. In fact, two of the participants specifically stated that they deliberately avoided using applications requiring personal details.

Detailed questions about the technical core components of IT security (integrity, availability, confidentiality and anonymity) were only touched on by the interviewees. This is no doubt because the EPCglobal network and the ONS service are still in the early stages of development, and also because it is believed in principle that known solutions from other application areas can be adopted to tackle these issues.

[25] The BIBA institute discussed a system for separating product and information costs [Uckel08].
„Controlled transparency“ could be created by implementing a billing system (based on readers fitted with a SIM card that would log and provide a cumulative calculation for read events). In this way, it would be possible to make some information freely available at no charge, while other information would be subject to charges and thus no longer freely available. Similarly, access could be restricted to some users, while others (e. g. competitors) could be excluded. Furthermore, by separating out costs, this proposal would also indirectly enhance the quality of the data/information because no-one wants to pay for useless information.

For most of the interviewees, integrity is an essential property of the EPCglobal network and its services. In particular, unambiguous assignment of EPC numbers to objects must be ensured, even if the ONS service is dispersed. On the subject of availability, the participants referred to the (known) deployment of mirrored ONS services, used to avoid a single point of failure. Only a few responses were returned regarding the importance of confidentiality and anonymity in the EPCglobal network, but most of these rated this importance as high.

Support by state agencies

Most of the interviewees saw no need for the ONS service or EPCglobal network to be either supported or regulated by state agencies. However, the companies that advocate state involvement are the very companies that accord a higher relevance to the EPCglobal network and ONS. These interviewees listed the following as desirable state involvement: support of alternatives to ONS, or of a transition to neutral deployment of the ONS and the future Internet of Things, plus coordination of discussion on ONS standardisation. At the same time, these interviewees spoke in favour of industry driving technology development. State-supported R+D projects were not considered appropriate. State support for early prototype solutions (first user action/early adopter initiatives) were considered appropriate however.

One interviewee was critical of the vague socio-political requirements surrounding self-regulation of network services like the ONS. In this individual's view, these requirements needed to be clarified by political representatives in collaboration with businesses and standardisation bodies.

5. Recommended actions

Finding

Companies that have already had been more deeply involved with ONS to date are more convinced of its future importance. However, they are concerned that alternative infrastructures may be suppressed prematurely, due to specifications or indeed by regulation.

Recommendation

Clarify the timing issue. Ensure that the Federal Government is in a position to respond quickly to increasing demand and the pace of European or international development.

Proposed operational measure

Establish a Federal Government watchdog body for the ONS/Internet of Things/Services. This body would produce a report on current developments and required actions either annually or biannually.

Finding

Owners of small and medium-sized businesses in particular, but also managers in large companies, either have no knowledge or only superficial knowledge of the ONS. They are therefore not aware of the challenges and possible implications of the ONS for their business processes. This is also why they are generally unable to articulate their interests in this area or present their functional requirements.

Recommendation

First and foremost, an information campaign is recommended, given the increasingly relevant role ONS is expected to play. Both large-scale and mid-sized companies should be informed of the possible standardisation plans and cost/benefit aspects of the new technologies.

Proposed operational measure

Launch an information campaign about the Internet of Things, in collaboration with scientific and industry bodies (e. g. AIM, BITKOM, Informationsforum RFID) and the relevant industry federations (e. g. GS1 Germany, VDA (automotive), VDMA (engineering) etc.) and influential research projects (e. g. ADiWa, SemProM, Aletheia[26] and BRIDGE[27]).

Finding

As a communications infrastructure, The Internet of Things is subject to the same threats and potential misuse as the existing Internet, with its trends towards Internet 2.0 or Web 3.0.

Recommendation

Minimise potential misuse associated with the identifiability of objects and consequent transparency of processes.

[26] ADiWa (Alliance Digital Product Flow; www.adiwa.net/), SemProM (Semantic Product Memory; www.semprom.org/) and Aletheia (Semantic Federation of Comprehensive Product Information; www.aletheia-projekt.de/) are current BMBF (Federal Ministry of Education and Research) research projects undertaken as part of the ICT2020 programme.

[27] BRIDGE (Building Radio Frequency IDentification for the Global Environment) is an integrated project supported by the EU that aims to overcome barriers to implementation of RFID solutions, based on GS1 EPCglobal standards (see http://www.bridge-project.eu/; last access on 11.12.08).

Proposed operational measure

Commission relevant research projects, extending the scope beyond the current work of the BRIDGE project and EPCglobal and examine medium to long-term issues regarding the Internet of Things.

Finding

Too little is known about the type of business cases that will actually require and prosper from an ONS. It is not yet clear which basic principles (generic components) need to be formulated and which (industry)specific solutions (individual components) will emerge.

Recommendation

Promote the development of best-practice industry solutions. The solutions that can produce the greatest number of „showcase“ examples will also be best placed in terms of introducing and enforcing standards.

Proposed operational measure

Early adopter initiative for SMEs. Promote industry-led cooperative projects that would award value chains using RFID/ONS for the first time and throughout the chain, thus setting an important example.

Finding

Industry (with the exception of large retailers) will not comment on the topic until something tangible is available for evaluation. This is a typical chicken-and-egg problem: Few companies want to be the first movers or work on a future infrastructure purely on an abstract level. Once an actual proposal is on the table, it will be examined and used, improved if necessary, or rejected. There is therefore a risk that structures will become rigidly set, without the input (or only unilateral input) of German companies.

Recommendation

Discuss the topic within the RFID roundtable.
The relevant associations must be included.

Proposed operational measure

Ensure that associations are included in relevant cooperative projects.

Finding

There is a lack of involvement among German industry representatives (particularly from small and medium sized enterprises) in standardisation debates and in the relevant bodies. Even larger businesses' participation in the work of standardisation bodies is rare, irregular or non-existent. The German industry sector is either not fully represented or not represented at all in debates at European level.

Recommendation

Enable the participation of German stakeholders in standardisation bodies and support standardisation projects. Avoid biased representation and act at a European level through mandating, e. g. through authorisation by the RFID roundtable.

Proposed operational measure

Give stimulus to standardisation projects in R+D projects and provide more generous funding (up to 100% if necessary). Restructure the RFID roundtable as an „Internet of Things“ discussion platform with a strict strategic focus.

Finding

The cost-benefit imbalance with RFID and in the expected Internet of Things acts as an obstacle to introduction via the value chain because suppliers mainly incur the costs, while later links in the value chain reap the benefits.

Recommendation

The costs must be distributed in line with information use. Care must also be taken to ensure that this information can only be used with appropriate authorisation, if this seems necessary. One of the ways of distributing costs to compensate fairly for expenditure would be to use a comprehensive billing system model, which would log and calculate read events from RFID tags, and allow access to be restricted to a particular user group (to be defined).

Proposed operational measure

It is as yet unclear whether the cost-benefit imbalance affecting RFID means that it is doomed to market failure now, or in the near future. Due to the potential damage this could cause, discussions should be held with the relevant sectors to determine if state regulation is required.

Finding

Most of the interviewees expect the infrastructure of the Internet of Things to avoid a monopoly, and be unbiased towards any particular industry or technology.

Recommendation

Timely strategies must be followed on the industry and technology-neutral implementation of the ONS and the Internet of Things and of their IT security. First, this will entail international agreement on the neutral standing of the EPCglobal network, especially within the European Union and with the US. Second, work should be carried out with the GS1 towards achieving the national anti-trust protection that may be required for the EPCglobal network (GS1 is an anti-trust law approved rationalisation association).

Proposed operational measure

Reach agreement among the participating divisions of the Federal Ministry for Economics (such as I B I Competition, regulatory and privatisation policy, VII C I General issues for the Information Society, IT, media, culture and creative industries and VII C 3 Development of convergent ICT) and subsequently hold discussions with GS1 in a German and international context.

General recommendation

A technical discussion of RFID/ONS and the Internet of Things should be held within the RFID roundtable. Some important additional contributors (e.g. from applied research) should be asked to join the roundtable.

Proposed operational measure

Hold an ONS session during next meeting of the roundtable or informal ONS discussion: Uckelmann on „Billing procedure“, Prof. Boche on „Communications technology“, Prof. Günther on „ONS infrastructure and ONS software“, Prof. Viola Schmid on „Internet law/ RFID“ etc.

Bibliography

[BKK03]
Hari Balakrishnan, M. Frans Kaashoek, David R. Karger, Robert Morris, and Ion Stoica. Looking up Data in P2P Systems. Communications of the ACM, 46(2): 43–48, 2003.

[BMWi07a]
Federal Ministry of Economics and Technology (BMWi). RFID: Prospectives for Germany.
The state of radio frequency identification-based applications and their outlook in national and international markets. Berlin 2007
[http://www.bmwi.de/ BMWi/Navigation/Service/publikationen,did=200776.html].

[BMWi07b]
Federal Ministry of Economics and Technology (BMWi). European Policy Outlook RFID.
Berlin, July 2007
[http://www.vdivde-it.de/Images/publikationen/dokumente/RFID-Konf-E.pdf].

[BMWi08]
Federal Ministry of Economics and Technology (BMWi). Reflection Paper of the Federal Government of Germany. From Berlin 2007 to Nice 2008 and Beyond: „RFID – Internet of Things – Internet of the Future“. Berlin 2008
[http://www.iotvisitthefuture.eu/fileadmin/docu-ments/roleofeuropeancommision/Reflections_on_ European_Policy_Outlook_RFID.pdf].

[BSI06]
Federal Office for Information Security (BSI).
RFID – Security Aspects and Prospective Applications of RFID Systems. Secumedia: Ingelheim 2006.

[BRI08]
EU BRIDGE Project, http://www.bridge-project.eu/.

[EFG08]
Sergei Evdokimov, Benjamin Fabian, and Oliver Günther. Multipolarity for the Object Naming Service. In Proc. Internet of Things (IOT 2008), Zurich, Switzerland, 2008, LNCS 4952, pages 1–18. Springer-Verlag, Berlin-Heidelberg, 2008.

[EC08]
Commission Staff Working Document. Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Future networks and the internet. Early Challenges regarding the „Internet of Things“. SEC(2008) 2516, Brüssel, 29.9.2008
[http://ec.europa.eu/information_society/policy/rfid/documents/earlychallengesIOT.pdf].

[EPC07]
EPCglobal. The EPCglobal Architecture Framework – Version 1.2, September 2007 [http://www.epcglobalinc.org/standards/architecture/].

[EPC08]
EPCglobal. EPCglobal Object Naming Service (ONS) 1.0.1, 2008
[http://www.epcglobalinc.org/standards/ons/].

[FAL06]
Patrik Fältström: RFID - Issues related to Internet and Regulation. A brief look at ONS and DNS, and Internet of Things. Workshop Interoperability, standardization, governance, and Intellectual Property Rights, Brüssel 1 Juni 2006 [www.rfidconsultation.eu/docs/ficheiros/au_conf670306_ fallstrom_en.pdf].

[FGS05]
Benjamin Fabian, Oliver Günther, and Sarah Spiekermann. Security Analysis of the Object Name Service. In Proc. 1st IEEE Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2005), in conj. with IEEE ICPS 2005, Santorini, Greece, pages 71–76, 2005.

[FG07]
Benjamin Fabian and Oliver Günther. Distributed ONS and Its Impact on Privacy. In Proc. IEEE International Conference on Communications (IEEE ICC 2007), Glasgow, 2007.

[FG09]
Benjamin Fabian and Oliver Günther. Security Challenges of the EPCglobal Network. Communications of the ACM, 2009.

[GS05]
Oliver Günther and Sarah Spiekermann. RFID and the Perception of Control: The Consumer's View. Communications of the ACM, 48(9):73–76, September 2005.

[LA06]
Cricket Liu and Paul Albitz. DNS and BIND. O'Reilly & Associates, 5th edition, 2006.

[Los04]
Pete Loshin. IPv6, Theory, Protocol and Practice. Elsevier, San Francisco, 2004.

[RFC2460]
S. Deering, and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460. December 1998.

[RFC4003]
Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose, „DNS security introduction and requirements," IETF, RFC 4033, 2005.

[Sol04]
Hesham Soliman. Mobile IPv6. Addison-Wesley, 2004.

[Uckel08]
Dieter Uckelmann, „The Value of RF-based Information," *in Dynamics in Logistics - First International Conference, LDIC 2007 Bremen, Germany, August 2007, Proceedings*, 1. Eded., H.D. Haasis, H.J. Kreowski and B. Scholz-Reiter, Edt, Springer, 2008, pp. 183-197.

Interview questionnaire

Has our introduction to the subject brought home the relevance of the ONS for you (for German industry, for your business)?

Are the five specified problem areas sufficiently comprehensive or do you believe there are other important issues to be tackled?

Unipolarity:

- Do you consider the current centralised infrastructure of the Internet of Things as problematic? If so, what is your main criticism/fear?
- What requirements would you impose on the infrastructure in terms of future organisation?
- How do you rate the measures to date on setting up national/regional ONS roots? Which problems are solved by these efforts, which problems remain the same and which problems are created (if applicable)?
- Can you think of alternative solutions?
- What implications would the alternatives have for you (compared to the existing system)? Is the risk that a business may become dependent on EPCglobal a serious argument against using ONS?

ONS-internal trust and power structures:

- In your opinion, who should have access to which data about your company's products?
- How should the control structures be established to ensure secure, trust-based access to the data?
- Which possible solutions are available within the framework of an operator model?

Integrity:

- Integrity and authenticity of data are obviously essential. In what ways could these be ensured, in your view?
- Which technical and organisational possible solutions do you know/do you prefer? In your view, what is the essential difference between DNS-based communication and DNS-based architecture?
- Are there exceptions for which the highest integrity requirements can be ignored?

Availability:

- Do you view the current, centralised ONS structure as a threat to the availability and functionality of the Internet of Things?
- Apart from the few (national/regional) ONS roots, are other architectures available that could offer a better guarantee of data availability and system stability?

Confidentiality and anonymity:

- Which types of confidentiality and anonymity are particularly important for your business?
- How important are technical issues in maintaining confidentiality and anonymity?
- Which organisational measures could be taken (e. g. assigning authorisations) in the Internet of Things to minimise the risk of misuse/criminal use?
- What are the possible alternatives to ONS-based communication in your view?

How would you compare the severity of the different possible problem areas? Which problems should be tackled as a priority, in your view?

Do you expect to see organisational changes if this type of Internet of Things comes into use (data modelling, IT management, workflow organisation, logistics, etc)? If so, can you specify these changes and describe the preparations you are making for them?

In your view, what are the minimum requirements to be met by a future infrastructure before you would favour your business participating in the Internet of Things?

What security-related requirements would you have of an infrastructure and related services?

Where do you see possible solutions to challenges relating to security and data protection? Which questions/issues have not yet been tackled or fully addressed?

Which system solutions and which application constellations are especially likely to be bound up with legal problems and issues (liability law, law relating to misuse etc.)?

Are you familiar with projects (committee work, R+D projects etc.) that tackle the possible problems discussed here?

What types of support would you like to see offered by the state in designing the infrastructure and accompanying security system for the Internet of Things? In fact, do you believe there is a need for regulation or do you have faith in the self-regulating ability of the market?

Do you see any particular need for support in relation to your own business/your customers?

Discussion participants

Interviewee	Role	Organisation	Sector
J. Bidlingsmaier	Project Manager Automotive	Seeburger AG	Car manufacturer software
R. Glatz	Managing Director of Professional Association Software and Industrial Communication	VDMA e.V.	Mechanical and plant engineering
W.-R. Hansen	Managing Director	AIM-D e.V.	RFID association
Dr. Sascha Henke	Business Planning	Robert Bosch GmbH, C/LP	Telemedicine/ medical technology
G. Leichert	Team Leader Automotive Projects	PSIpenta GmbH	Software and solution provider
G. Peeters	Operations Manager	CBR Fashion Holding GmbH	Textile industry branded goods
U. Quiede	RFID Project Manager	Kaufhof Warenhaus AG	Retail department store chain
M. Scheferhoff	Program Manager RFID Lufthansa Technik Group	Lufthansa Technik Logistik GmbH	Logistics
D. Spannaus	IBM Managing Consultant, IBM Interactive	IBM Deutschland GmbH	Software and solution provider
M. Sprafke	Director of Quality Planning and Field Data Analysis	Volkswagen AG	Car manufacturer
R. Tröger	RFID Project Lead	Gerry Weber International AG	Textile industry branded goods
D. Uckelmann	Researcher	University of Bremen	Scientific research (logistics)

This Report is published as part of the public relations work of the Federal Ministry of Economics and Technology. It is distributed free of charge and is not intended for sale. It may not be used by political parties or canvassers during an election campaign for the purpose of canvassing. In particular, distributing the Report at election meetings or on political parties' information stands, inserting party political information or advertising, or printing or attaching such information onto the Report are regarded as misuse. Similarly, the Report may not be transferred to third parties for the purposes of electioneering. Regardless of how, when or in what quantity this Report reaches the recipient, it may not be used, even outside the timeframe of an election, in a way that could be construed as Federal Government support for individual political groups.