Bundesministerium
für Wirtschaft
und Technologie

Dokumentation
Nr. 581

Dokumentation

Internet der Dinge

Leitfaden zu technischen, organisatorischen, rechtlichen und sicherheitsrelevanten Aspekten bei der Realisierung neuer RFID-gestützter Prozesse in Wirtschaft und Verwaltung

www.bmwi.de

Redaktion:
Alfons Botthof, Institut für Innovation + Technik
in der VDI/VDE-IT GmbH (Projektleitung)
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, Institut für Innovation + Technik
in der VDI/VDE-IT GmbH

Produktion/Druck
Harzdruckerei GmbH Wernigerode

Herausgeber
Bundesministerium für
Wirtschaft und Technologie
Referat Öffentlichkeitsarbeit
10115 Berlin
www.bmwi.de

Stand
Mai 2009

Das Bundesministerium für Wirtschaft und Technologie ist mit dem audit berufundfamilie ® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Bundesministerium
für Wirtschaft
und Technologie

Dokumentation

Internet der Dinge

Leitfaden zu technischen, organisatorischen, rechtlichen und sicherheitsrelevanten Aspekten bei der Realisierung neuer RFID-gestützter Prozesse in Wirtschaft und Verwaltung

Für den eiligen Leser!

Neben dem Barcode etabliert sich zunehmend die **RFID-Technologie zur Identifikation von Objekten** aller Art. Die eindeutige Identifizierung in Verbindung mit der Möglichkeit, zusätzliche mit dem Objekt verknüpfte Informationen an jedem Ort und zu jeder Zeit verfügbar zu machen, hat bereits heute zu effizienten Prozessen, neuen Produkten und innovativen Dienstleistungen geführt. Werden die Objekte zusätzlich mit sensorischen Fähigkeiten und Lokalisierungsoptionen – beispielsweise durch GPS – ausgestattet, sind auch **autonome, quasi-intelligente Anwendungen** möglich, die auch eine vernetzte Objekt-zu-Objekt-Kommunikation einschließen können (**smarte, interagierende Objekte**). Alle diese Anwendungen, die auf dem Einsatz heutiger und künftiger Identifikationstechnologien basieren, sind essentiell darauf angewiesen, dass die **Kommunikation und die Zugriffe auf Datenbasen zuverlässig, sicher und integer** geschehen. Dieser hohe Anspruch an die Informations- und Kommunikationstechnologien muss insbesondere dann kompromisslos erfüllt werden, wenn Daten in offenen, also äußeren Gefährdungen ausgesetzten Netzen übertragen werden. Nur so können die für eine erfolgreiche Einführung unabdingbare Akzeptanz und das notwendige Vertrauen von Kunden, Anwendern und Nutzern in Wirtschaft und Gesellschaft erreicht werden.

Die hier vorgelegte Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie zeigt wesentliche **technische Verfahren zur Organisation anspruchsvoller, internetbasierter Kommunikationsprozesse für das Internet der Dinge** auf. Sie konzentriert sich beispielhaft auf die als ONS (**O**bject **N**aming **S**ervice) bekannte Thematik (**Verwaltung und Zugriff auf das grundlegende Verzeichnis von Objektidentifikatoren und Abfrage dezentral abgelegter Beschreibungsdaten**) und erhebt nicht den Anspruch, umfassende Überlegungen zu Fragen der Governance (Verwaltungshoheit, Schutz von Daten und Rechte Betroffener) einer künftigen Infrastruktur des Internets der Dinge anzustellen.

- **Manager, hier insbesondere IT-Verantwortliche in Unternehmen, werden zu den technischen, organisatorischen, rechtlichen und sicherheitsrelevanten Aspekten und deren Implikationen beim Einsatz von Identifikationstechnologien sensibilisiert und erhalten wertvolle Hinweise und Anregungen, wie RFID-basierte Prozesse sicher, das heißt zuverlässig und integer, in IT-Lösungen heute umgesetzt werden können. An innovationspolitische Akteure werden Empfehlungen basierend auf Expertengesprächen mit Stakeholdern ausgesprochen.**

Die Kenntnis über grundsätzliche Informations- und Kommunikationsprozesse, die mit der Einführung der Technologie in Produkten, Prozessen und damit verbundenen Dienstleistungen zu realisieren sind, ist für **Verantwortliche in Unternehmen eine zentrale Voraussetzung, gemeinsam mit Partnern in der Wertschöpfung den nächsten Entwicklungsschritt hin zum Internet der Dinge erfolgreich beschreiten zu können**. Der vorliegende Leitfaden will hierfür wichtige Hinweise liefern und zeigt Möglichkeiten und Grenzen auf.

Einschätzungen[1] auf einen Blick

heute	morgen
Barcode (Strichcode, 2D) RFID-Systeme (Lesegeräte, Etiketten), vereinzelt RFIDs mit integrierter Sensorik	Barcode (Strichcode, 2D, 3D) Vermehrt energieautarke, vernetzbare RFID-Etiketten mit Sensorfunktionalitäten
IPv4	IPv6
Zentralisierte Vermittlungsstelle (ONS) zwischen Objektcode und (Produkt-)Informationsdatenbasen	Dezentral organisierte Services (regionale ONS-Architekturen, Peer-to-Peer-Architekturen)
Unipolares ONS	Multipolares ONS
EPCglobal-Netzwerk (vornehmlich für den Handel)	EPCglobal und weitere sektorspezifische Netzwerke
Einheitlicher Standard EPCglobal und Gewährleistung der Eineindeutigkeit des EPC-Nummernkreises	Sektorspezifisch erweiterte Standards, aber weiterhin Eineindeutigkeit des EPC-Nummernkreises
Geringe Skalierbarkeit von ONS	Hohe Skalierbarkeit von ONS
IT-Risiken (z. B. Datenintegrität, -authentizität, -verfügbarkeit, -vertraulichkeit)	Neue Verfahren zur Minderung der IT-Risiken und Verbesserung der IT-Sicherheit
Zentral organisierte und verwaltete globale Sicherheitsinfrastruktur	Dezentral organisierte und verwaltete Sicherheitsinfrastruktur
Mangelhafte Strategieverfolgung auf europäischer Ebene zu künftiger Machtstruktur und Governance	Wirtschafts- und technologiepolitisch neutrales ONS; Europäische Abstimmungen zu Governance-Strukturen
Unzureichende Transparenz über technische und politische Entwicklungen im Kontext „Internet der Dinge“	Etablierter Internet der Dinge/Dienste-„Watch“ im Auftrag deutscher Stakeholder
Unzureichende Vertretung deutscher Interessen in internationalen Standardisierungsgremien; keine neutrale Standardisierung	National abgestimmte Standardisierungsstrategie und Unterstützung mittelständischer Interessensvertretung
Eher „abstrakte“ Mitarbeit an künftiger Infrastruktur	Mitarbeit an Infrastruktur auf dem Hintergrund von Anforderungen in konkreten Vorhaben
Geringe strategische Bedeutung für Unternehmen (insb. Mittelstand) (Festhalten an bewährten Lösungen; Ausnahme: Handel)	Hohes Potenzial operativ wie strategisch Ablösung veralteter EDI-Strukturen
Unzureichende Vorbereitung betroffener Unternehmen auf Herausforderungen und Potenziale von ONS bei dessen Einführung	Breit, d.h. von vielen stakeholdern getragene Informationskampagne
Geringe Kenntnis über „use cases“ für ONS	Erfahrungswerte durch branchenspezifische, beispielgebende Lösungen
Unklarheit über Kosten-Nutzensituation	Beispielhaft kalkulierte use cases zur Orientierung für Anwender
Hohe Kosten für Sevices aufgrund quasimonopoler Strukturen	Kostenreduktion durch Wettbewerb
Einfache, unflexible Gebührenmodelle	Flächendeckendes Billingsystem (Mikro-Payment pro Datenzugriff resp. Leseereignis)
Kundenprofilbildung kaum möglich in „closed-loops“	Profiling erleichtert in offenen Prozessen unter Einschluss des Endkunden

[1] Diese Einschätzungen stammen von den Fachexperten (siehe Liste S. 52), die sich im Rahmen der Studie für ausführliche Interviews zur Verfügung stellten.

Wir danken allen Gesprächspartnern aus Wirtschaft und Wissenschaft für ihre Bereitschaft, sich auf das Thema ONS eingelassen, sich teilweise intensiv damit befasst und uns für die ausführlichen Interviews zur Verfügung gestanden zu haben. Ebenfalls gedankt sei den Mitgliedern des Dialogkreises RFID für ihre konstruktiven Anregungen.

Inhalt

1. Einleitung, Zielstellung und Design der Studie

Im Zusammenhang mit der Begleitforschung zu NextGenerationMedia wurde deutlich, dass das Thema RFID und der sich ankündigende Evolutionsschritt in Richtung eines „Internet of Things“ und eines „Internet of Services“ in der gegenwärtigen Diskussion eng mit dem EPCglobal Network und dem Object Naming Service (ONS) verbunden ist. Der ONS dient als grundlegendes Verzeichnis für die Zuordnung der im RFID-Tag gespeicherten Kennung (Identifikator) mit hierzu hinterlegten Informationen. Für den im Bereich Handel und Konsumgüter maßgeblichen EPC (Electronic Product Code) erfolgt der Betrieb des ONS im Auftrag von GS-1/EPCglobal durch die Firma VeriSign in den USA. Daraus ergibt sich, dass nach dem bestehenden Betreibermodell der weltweite Zugriff auf die mittels RFID adressierten Daten zentral über einen in den USA lokalisierten Server geschieht.

In Politik, Wissenschaft und Wirtschaft wurden bereits mehrfach Vorbehalte gegenüber einer derart zentralisierten (monopolisierten) Infrastruktur und damit Abhängigkeit formuliert. Der grundsätzlich mögliche Missbrauch durch eine zentrale Kontrolle von Waren- und Informationsflüssen, wie z. B. der Zugang zu vertraulichen Logistikdaten, wird dabei unter Konkurrenzgesichtspunkten für nicht akzeptabel gehalten. Besonders schwerwiegend sind die Bedenken, wenn es sich statt um elektronische Produkt-Codes für Konsumgüter um Daten handelt, die der staatlichen Souveränität (z. B. Raumfahrt, Verteidigungsbereich) unterliegen. Die Verwaltung solcher für den Staat vitaler Datenströme wird aus Gründen der Sicherheit, Verfügbarkeit und Exklusivität nur sehr bedingt für auf Dritte übertragbar gehalten.

Die bisher nur unzureichend beantwortete Frage nach der Gewährleistung staatlicher Souveränität und Sicherheit der Infrastruktur und die Tatsache, dass gegenwärtig der erste europäische EPC Root ONS in Europa in Frankreich installiert wird, zeigt, dass dem Thema ONS und damit der Organisationsstruktur des Internet der Dinge eine wachsende Bedeutung zukommt.

Es wird sich zeigen, ob dem künftigen Internet der Dinge eine ähnliche Entwicklung zuteil wird, wie es das heutige Internet durch WWW und HTML erfuhr. Es ist für die Zukunft zu erwarten, dass entsprechende Dienste zur Zuteilung bzw. Abfrage von Identifikatoren auch jedem privaten Internetnutzer den Zugriff auf neue Objekte ermöglichen. Solche Modelle verlangen verstärkt Antworten auf die Fragen: Wer hat Zugriff auf welche Daten? Wer darf welche Daten zu welchen Objekten hinterlegen? Wie werden die angebotenen Leistungen bezahlt? Wie kann Hoheit über die Daten gewährleistet werden? Wie kann den Ansprüchen nach Sicherheit, Datenschutz und Verbraucherschutz Rechnung getragen werden?

Auch die weiteren Entwicklungsstufen (Stichwort ONS 2.0 oder IPv6, peer2peer) bedürfen einer fachlichen Bewertung sowie Überlegungen zum Timing der Einführung neuer technisch-organisatorischer Lösungen für das Internet der Dinge und der Dienste. In die Betrachtungen sollte insbesondere die Rolle von IPv6 beim Internet der Dinge und die Identifikation eines möglichen Handlungsbedarfs einbezogen werden. Konkrete Szenarien in potenziellen Anwenderbranchen werden dabei behilflich sein, die Tragfähigkeit der verschiedenen Ansätze aus organisatorischer und sicherheitstechnischer Sicht diskutieren zu können.

Um die Einflussmöglichkeiten und Handlungsoptionen von Wirtschaft und Politik im Hinblick auf die technische Konzipierung/Umsetzung eines solchen Systems und die Schaffung eines angemessenen Rahmens einschätzen zu können, wird im Rahmen der Begleitforschung zu NextGenerationMedia diese Kurzstudie erstellt. Sie soll insbesondere den gegenwärtigen Grad der Sensibilität gegenüber den o. a. Fragen und die Bedarfslage der heimischen Industrie exemplarisch erfassen.

Die vorliegende Studie diskutiert diese Problematik in einem interdisziplinären Kontext unter Berücksichtigung der relevanten technologischen, infrastrukturell-organisatorischen sowie ökonomischen, rechtlichen und sicherheitsrelevanten Herausforderungen. Dabei wird Wert darauf gelegt, nicht nur den Sachstand hinsichtlich ONS darzustellen, sondern anhand von Interviews qualifizierte Einschätzungen von hochrangigen Entwicklern und Anwendern im Feld EPCglobal Network / Internet der Dinge einzuholen, um so zukünftige Ausprägungen des ONS und alternative Entwicklungen zu skizzieren.

Dabei ist es wichtig, in Ergänzung der laufenden einschlägigen Initiativen deutscher Unternehmen, die sich im Wesentlichen auf die Betrachtung eines Zwei-Jahres-Horizonts konzentrieren, eine längerfristige Perspektive einzunehmen. Die Transformation des Internets der Dinge und der Dienste von einer prototypischen Implementierung zur einer kritischen Infrastruktur wird sich wohl erst in fünf bis zehn Jahren vollziehen. Eine solche Transformation verläuft aber im Regelfall nicht linear, sondern sprunghaft. Entwurfsentscheidungen, die jetzt getroffen werden, können hierbei plötzliche und gravierende Konsequenzen haben. Daher ist es wichtig, diese Entwurfsentscheidungen jetzt und vor einem politisch-ökonomischen Hintergrund kritisch zu überprüfen.

Es gilt insbesondere die Frage zu beantworten, ob basierend auf den Projektergebnissen von NextGenerationMedia zusätzlicher staatlicher Handlungsbedarf im Hinblick auf Unternehmensinteressen bzw. zum Schutz der deutschen Wirtschaft vorliegt. Diese Studie soll also dazu beitragen, die Interessen der deutschen Wirtschaft im Dialog mit wissenschaftlichen Experten aufzunehmen und zu bewerten, soll Empfehlungen zur „Governance“ aussprechen und soll mögliche technologiepolitischen Initiativen anstoßen helfen.

Für eine solche Initiative ist es keineswegs zu früh, auch wenn das Thema bei vielen Unternehmen derzeit noch nicht die allerhöchste Priorität genießt. Die Frage ist nicht, ob das Internet der Dinge und der Dienste Realität wird – dies wird mittelfristig zweifelsohne der Fall sein. Die Frage ist vielmehr, wie man den Weg dorthin möglichst effizient gestalten kann – und dies in einer Weise, die für die deutsche bzw. europäische Volkswirtschaft insgesamt den größten Nutzen verspricht. Vor diesem Hintergrund ist es essenziell, ONS und das Internet der Dinge als eine in Zukunft wichtige Infrastruktur zu verstehen, deren Auswirkungen auf die Zuverlässigkeit und Sicherheit nationaler Strukturen vorab gründlich zu analysieren und auch aus ordnungspolitischer Perspektive fundiert zu evaluieren.

Das Kapitel 2 führt kurz in das Konzept des ONS im EPCglobal Network und die gegenwärtige Diskussion um den Object Naming Service ein. Die Abschnitte 2.1 bis 2.3 dieses Kapitels wurden den Gesprächspartner vorab als Themenaufriss und Interviewleitfaden zur Verfügung gestellt. Kapitel 3 analysiert die gegenwärtige ONS-Spezifikation hinsichtlich ihrer Herausforderungen bei Technik, Organisation und IT-Sicherheit. Ebenso werden aktuelle Alternativ- und Ergänzungsvorschläge wie Multipolares ONS, Peer-to-Peer ONS und DNSSEC diskutiert. Die im Rahmen dieser Studie geführten Interviews mit den Experten aus Industrie und Verbänden werden in Kapitel 4 zusammengefasst. Kapitel 5 leitet aus den Analysen und Interviews Handlungsempfehlungen für die Bundesregierung ab.

2. Einführung in das EPCglobal Network und den ONS

2.1 Aufgabe eines Namensdienstes für das Internet der Dinge

Die Grundidee der Radiofrequenzidentifikation (Radio Frequency Identification, RFID) besteht in der Assoziation physischer Objekte mit kleinen und preisgünstigen Computerchips (sogenannten *Tags*), die ohne Sichtkontakt über Funk ausgelesen werden können.

Die Tags speichern typischerweise weltweit eindeutige Kennungen (*Identifikatoren*) der Objekte, mit denen sie assoziiert sind. Die wohl wichtigste Konvention für derartige Identifikatoren ist der sogenannte *elektronische Produktcode* (*Electronic Product Code, EPC*), der vom Industriekonsortium EPCglobal spezifiziert wurde. EPCs sind ein global verfügbares und weltweit eindeutiges Nummernsystem zur Benennung von Objekten. Ein Beispiel für einen EPC ist in Abb. 1 dargestellt.

Abbildung 1: Beispiel für einen EPC

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

Hier repräsentiert der erste Teil (*Company Prefix*) die Kennung des Unternehmens, das das fragliche Objekt hergestellt hat. Der zweite Teil (*Object Class*) bezeichnet die Art des Objekts (z. B. eine bestimmte Art von Kleidungsstück). Der dritte Teil, die Seriennummer (*Serial Number*), repräsentiert eine ganz wesentliche Neuerung gegenüber dem herkömmlichen Barcode. Mit dieser Seriennummer lassen sich unterschiedliche Instanzen derselben Produktklasse unterscheiden, wie z. B. unterschiedliche Hosen des gleichen Herstellers und gleicher Art und Größe.

Produkt- und Logistikdaten zu einem konkreten Objekt werden im Allgemeinen nicht direkt auf dem RFID-Tag gespeichert, sondern in vernetzten Datenbanksystemen der unterschiedlichen Logistikpartner abgelegt, wobei der EPC als Suchschlüssel für Informationen dient. Diese Datenbanken können weltweit verteilt sein und auch über das Internet als *EPC-Informationsdienste* (*EPC Information Services, EPCIS*) angesprochen werden. Zusammen mit weiteren Diensten wird diese globale Informationsarchitektur auch als „Internet der Dinge“ bezeichnet. Als solche bildet sie eine Vorstufe und zukünftige Ergänzung eines Internets aus direkt vernetzten „Smart Objects“ (etwa auf Basis des IPv6-Protokolls).

Zentraler Akteur bei der Standardisierung des EPC und der zugehörigen Informationsarchitektur ist das internationale Industriekonsortium *EPCglobal*, das mit dem *EPCglobal-Netzwerk* eine konkrete, privatwirtschaftlich organisierte Version des Internet der Dinge zu betreiben plant.

Wie gelangt man nun von einem EPC, d. h. der eindeutigen Kennung eines Objekts, zu den zugehörigen objektspezifischen Informationen, also insbesondere den relevanten EPC-Informationsdiensten? Diese Aufgabe übernehmen Namens- und Suchdienste, wie der so genannte *Objektnamensdienst* (*Object Naming Service, ONS*) und sogenannte *Entdeckungsdienste* (*Discovery Services*). Für den ONS liegen bereits recht detaillierte Spezifikationen vor, die in der vorliegenden Studie ausführlich analysiert werden. Für die Entdeckungsdienste liegen noch keine derart detaillierten Spezifikationen vor.

2.2 Funktion des Object Naming Service

Wenn mithilfe eines RFID-Lesegeräts der EPC eines Gegenstands erfasst wird, hat man damit noch keinen Zugriff auf die objektrelevanten Informationen. Hierzu ist es vielmehr erforderlich, die zugehörigen Informationsdienste (EPCIS) im Internet zu lokalisieren und zu konsultieren. Das ONS stellt das hierfür erforderliche Verfahren für die „Auflösung" von EPCs zu Internetadressen der relevanten EPCIS (in Form von URLs) bereit.

Konzeptionell kann ONS als ein verteiltes hierarchisch organisiertes Informationssystem angesehen werden. Die höchste Ebene der Hierarchie (der *ONS-Wurzelknoten* bzw. *ONS-Root*) enthält die Adressen der Knoten auf der zweiten Ebene (EPC-Manager), die z. B. von Produzenten oder Großhändlern betrieben werden und für einen bestimmten Bereich von EPCs verantwortlich sind. Die EPC-Manager enthalten ihrerseits die Adressen von EPCIS, die Schnittstellen zu Datenbanken darstellen, in denen die relevanten Produkt- und Logistikdaten gespeichert sind.

Abbildung 2: Abfrageprozess im ONS

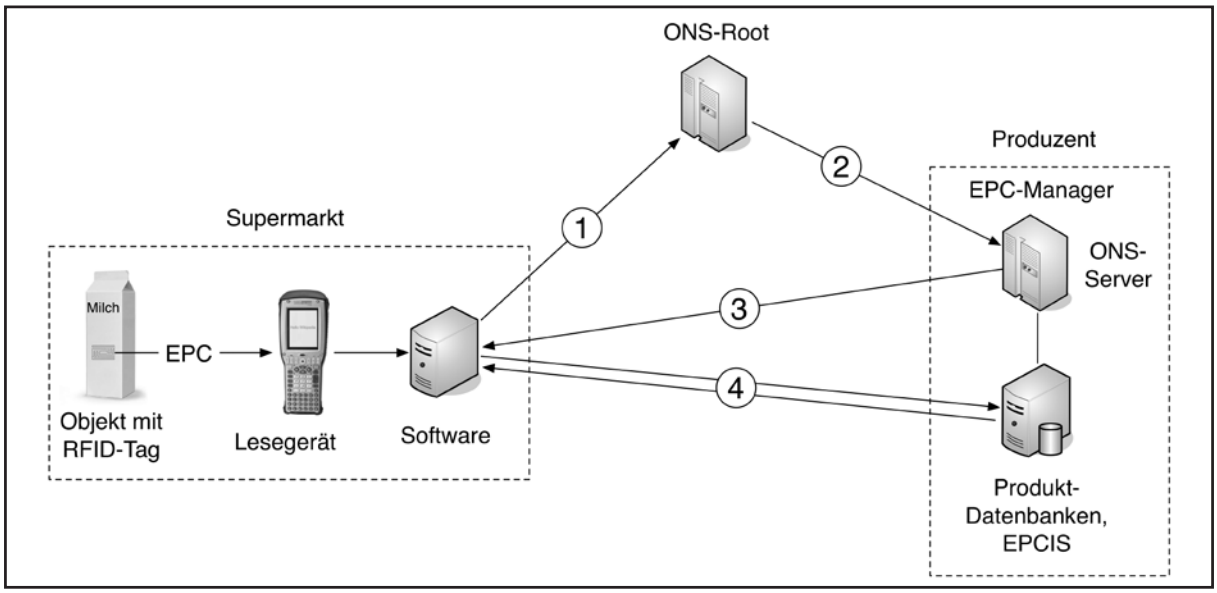


Abbildung 2 skizziert ein vereinfachtes Beispielszenario. Hier wird in einem Supermarkt ein an einer Milchtüte angebrachter RFID-Tag ausgelesen. Um die für die fragliche Milchtüte relevanten Daten aus dem „Internet der Dinge" zu extrahieren, wird mittels einer Spezialsoftware (Middleware) die Anfrage an den ONS-Wurzelknoten geschickt (Schritt 1). Der ONS-Wurzelknoten delegiert die Anfrage zum ONS-Knoten des EPC-Managers, d. h. zur ONS-Infrastruktur des Unternehmens, das die Milchtüte (und/oder die darin enthaltene Milch) produziert hat (Schritt 2). Der bzw. die zuständigen ONS-Server des EPC-Managers senden die Internetadressen der EPCIS, die relevante Produktdaten enthalten könnten, an die anfragende Partei zurück (Schritt 3). Mithilfe dieser Adressen können bei den EPCIS die Produkt- und Logistikdaten für den gelesenen EPC abgefragt werden, wobei ggf. Zugriffseinschränkungen geltend gemacht werden können (Schritt 4).

Durch das Caching von Ergebnissen vorheriger Anfragen können die Adressen des entsprechenden ONS-Servers oder sogar des EPCIS schon bekannt sein. In diesen Fällen könnten der ONS-Server oder der EPCIS auch direkt kontaktiert werden, ohne dass der ONS-Root einbezogen wird. Wenn aber die entsprechenden Adressen noch nicht im Cache enthalten sind, oder der Cache nicht mehr aktuell ist, wird die Abfrage so verlaufen, wie in Abbildung 2 dargestellt.

2.3 Herausforderungen des ONS

2008 werden weltweit wohl mehr als zwei Milliarden RFID-Tags verkauft werden, eine Zahl, die sich bis 2016 auf schätzungsweise 500 Milliarden erhöhen könnte.[2] Je mehr Firmen und auch Privatpersonen RFID einsetzen werden, desto stärker wird die Bedeutung des ONS als globalem Vermittler für RFID-Informationen zunehmen. Deshalb ist es von entscheidender Bedeutung, den ONS effizient, sicher und wohl definierten Fairnesskriterien genügend zu gestalten.

Ein erster technischer ONS-Standard ist bereits von EPCglobal veröffentlicht und ratifiziert worden. Wenn man allerdings – analog zum klassischen Internet – die wichtige zukünftige Rolle des ONS für die weltweiten Handelsbeziehungen und die voraussichtlich zunehmende Abhängigkeit der nationalen Ökonomien vom ONS in Betracht zieht, so ist es absolut essenziell, diesen ONS-Entwurf nicht nur aus einer technischen Perspektive zu evaluieren, sondern auch seine ökonomischen und politischen Implikationen zu überprüfen.

Eine Hauptaufgabe des ONS besteht darin, kooperierenden Teilnehmern einer Wertschöpfungskette einen standardisierten Weg zu eröffnen, um hohe Aufkommen von detaillierten Informationen über den Status und die Bewegung von Gütern untereinander auszutauschen. Dies kann mittelfristig zu signifikanten Effizienzgewinnen in den heute allerorten vorhandenen komplexen Wertschöpfungsketten führen, insbesondere indem die Transparenz der Prozesse und Güterflüsse zu einer besseren Planung und Optimierung logistischer Prozesse genutzt wird. Insofern ist die Frage nicht, ob das Internet der Dinge Realität wird – dies wird mittelfristig zweifelsohne der Fall sein. Die Frage ist, wie man den Weg dorthin möglichst effizient gestalten kann – und dies in einer Weise, die für die deutsche bzw. europäische Volkswirtschaft insgesamt den größten Nutzen verspricht.

Vor der Realisierung der zu erwartenden Effizienzgewinne sind diverse Adaptionshindernisse zu überwinden – hierzu gehören u. a.

- die ungleiche Verteilung von Kosten und Nutzen einer ONS-Infrastruktur unter den an einer Wertschöpfungskette beteiligten Partnern;

- die oft erst mittel- oder langfristig erzielbare betriebswirtschaftliche Rentabilität einschlägiger Investitionen sowie

- „lock-in"-Situationen für Unternehmen, wenn sie in eine zu große Abhängigkeit vom ONS gelangen – und damit auch von den Geschäftsstrategien von EPCglobal und den mit dem Betrieb des ONS beauftragten Unternehmen.

Vor diesem Hintergrund ist für Deutschland und andere Länder von Bedeutung, ONS und das Internet der Dinge als eine zukünftige IT-Infrastruktur zu verstehen, deren Auswirkungen auf die Zuverlässigkeit und Sicherheit nationaler Strukturen vorab gründlich zu analysieren und auch aus ordnungspolitischer Perspektive fundiert zu evaluieren.

ONS-interne Machtstrukturen

Das ONS-Root hat die Kontrolle darüber, an welche EPC-Manager die Anfrage weitergeleitet wird, und stellt einen kritischen Vermittlungspunkt im globalen System dar, der die Informationssuche für alle Produkte weltweit betrifft. Der EPC-Manager hat die Hoheit darüber, welche seiner eigenen EPCIS mit ONS gefunden werden können, sein Einflussbereich ist somit im Vergleich zum ONS-Root eingeschränkt auf Informationen zu seinen eigenen Produkten.

Bei der Suche nach beliebigen relevanten EPCIS für ein Objekt (also auch unabhängig vom jeweiligen Hersteller betriebene) sollen die noch nicht spezifizierten EPCIS-Discovery Services eine wichtige Hilfestellung leisten.

[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

Der Hauptbetreiber des ONS-Roots, VeriSign, ist ein Unternehmen, das der Gesetzgebung der USA untersteht, was für eine internationale Infrastruktur von derartiger Kritikalität nicht unproblematisch erscheint. Es ist derzeit noch ungewiss, ob andere Staaten dem Vorbild Frankreichs folgen (vgl. 3.1.1.2) und eigene ONS-Wurzelknoten betreiben werden, und wie unabhängig diese in der Praxis von VeriSign sein können. Offene Fragen betreffen u. a. die Koordination und den Datenabgleich zwischen den (vielen?) Wurzelknoten und die Verwaltung der ONS-Wurzeldatei sowie die Integrierbarkeit alternativer Architekturen für einzelne Länder oder Regionen.

Integrität

ONS benutzt das etablierte DNS- (Domain Name System) Protokoll des Internets, bei dem alle Nachrichten im Klartext und meist auf Basis des zustandslosen User Datagram Protocol (UDP) versendet werden, das aus Geschwindigkeitsgründen keine Fehlererkennung oder Sequenznummern für Nachrichten benutzt. Die dem DNS eigenen Identifikationsnummern zur Zuordnung von Anfrage und Antwort sind ungeeignet, um in der Praxis zu verhindern, dass die Kommunikation oder sogar in bestimmten Fällen die DNS-Daten auf den Servern selbst von Dritten gefälscht werden kann.[3] So können etablierte Angriffsmuster, z. B. Man-in-the-Middle-Angriffe oder Cache Poisoning einfach auf das ONS übertragen werden. In der jetzigen ONS-Spezifikation gibt es keine Möglichkeit zur Gewährleistung von Integrität und Authentizität der Adressdaten.

Ein bewährtes Paradigma bei der IT-Sicherheit ist die Tiefenstaffelung von Verteidigungsmechanismen (Defense-in-Depth Prinzip), demzufolge einem potenziellen Angreifer möglichst viele Hürden in den Weg gelegt werden sollten. Deshalb sollte die Absicherung der Integrität nicht ausschließlich auf die EPCIS-Kommunikation verlagert werden, was auch nicht genügen würde: Fälscht man die Zuordnung von EPC zu URL im ONS, so hat man im Allgemeinen keine Möglichkeit, z. B. anhand des SSL-/TLS-Zertifikats des EPCIS, das ja korrekt ausgestellt sein kann (aber nur die korrekte Zuordnung von URL zu Identität belegen kann), festzustellen, dass man nicht den korrekten Kommunikationspartner zu diesem EPC angesprochen hat.

Verfügbarkeit

Das ONS-Root stellt einen „Single Point of Failure“ dar: Die im Vergleich zum Gesamtsystem geringe Anzahl zentraler ONS-Root-Server muss im Zeitalter von sogenannten „Bot“-Netzwerken, die teilweise aus Hunderttausenden von infizierten und ferngesteuerten Computern bestehen, mit konzertierten, massiven Angriffen durch zahllose parallele Anfragen rechnen, die den Betrieb stören können (Distributed Denial-of-Service). Es bedarf weiterer Forschung, um abschätzen zu können, ob gegenwärtige Replikationsmaßnahmen beim DNS diesen neuartigen Bedrohungen auch in Zukunft gewachsen sein werden.

Vertraulichkeit und Anonymität

Auf Basis des DNS ist keine Gewährleistung von Vertraulichkeit der ONS-Daten möglich. Selbst wenn die eigentliche EPCIS-Kommunikation authentifiziert und verschlüsselt wird, so können Anfragen von Nutzern an das ONS einfach von allen Servern, dem ONS-Root oder auch jedem Internet-Service-Provider mitgelesen und samt Ursprungsadresse, die oft orts- oder personenbeziehbar ist, mitprotokolliert werden. Jede ONS-Anfrage von Firmen oder Personen betrifft Objekte der realen Welt und könnte zur Identifizierung, Profilbildung (Besitz, Beziehungen) und eventuellen groben Ortung der Nutzer eingesetzt werden – analog zu RFID-Datenschutzproblemen, wahrscheinlich weniger granular als durch RFID-Lesegeräte, dafür aber im globalen Maßstab bei großen Nutzergruppen. Dies betrifft auch Firmen, deren Logistik und Beschaffungsstrategien für Dritte transparent werden könnten.

[3] Im Sommer 2008 wurde dieses Problem auch in den Massenmedien diskutiert, z. B. Spiegel-Online vom 7.8.2008, „Wie ein Riesenloch im Netz die Sicherheit bedroht“: http://www.spiegel.de/netzwelt/web/0,1518,570584,00.html; letzter Zugriff 12.11.2008

2.4 Die politische Diskussion um den ONS

Die Herausforderungen des EPCglobal Network und des ONS an die Wirtschafts- und Technologiepolitik sind früh erkannt worden. Bei der politischen Debatte um den ONS-Dienst lassen sich zwei Diskussionsstränge identifizieren: die Governance des Dienstes einerseits und die Sicherheit des Dienstes und des EPCglobal-Netzwerks andererseits.

Bereits kurz nach der Verabschiedung der ersten stabilen ONS-Spezifikation im Jahr 2005 [EPC05] äußerten sich erste Experten zur Governance des zukünftigen ONS-Dienstes. Patrik Fältström (Cisco) wies auf einem Workshop im Rahmen des RFID-Konsultationsprozesses der Europäischen Kommission auf die Gefahr einer möglichen Monopolisierung des EPCglobal-Netzwerk durch den Betreiber des ONS-Dienstes hin [Fal06]. Mögliche IT-Sicherheitsrisiken des EPCglobal-Netzwerks wurden seit etwa 2003 im akademischen Umfeld prinzipiell thematisiert, etwa in der BSI-Studie *Risiken und Chancen des Einsatzes von RFID-Systemen* [BSI04].

In die politische Diskussion eingebracht wurden die Governance und die Sicherheit des ONS-Dienstes dann durch das Communique der Europäischen Kommission *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* im März 2007 (EC 2007). Gefordert wurden ein integrierter Schutz von Privacy und IT-Sicherheit in RFID-Systemen sowie die Offenheit und Neutralität „of the databases that will register the unique identifiers that lie at the heart of the RFID system". Um einen Dialog zwischen allen relevanten Interessensgruppen zu führen, wurde von der Kommission eine zweijährige RFID Expert Group aufgesetzt, die die Kommission bei der Gestaltung ihrer RFID-Politik beraten sollte. Die Gruppe hat sich vor allem mit der Erarbeitung eines Kompromisses zum Datenschutz bei RFID-Systemen beschäftigt. Arbeitsergebnisse wurden bislang nicht veröffentlicht. Daneben hat die Kommission mehrere Forschungsprojekte aufgesetzt, die sich mit den technischen Fragen der Sicherheit des EPCglobal-Netzwerks beschäftigen, insbesondere das Projekt BRIDGE, an dem mehrere GS1-Organisationen beteiligt sind.

Die Themen Governance und Sicherheit des ONS-Dienstes wurden auch in der Auftragsstudie des BMWi *RFID: Potenziale für Deutschland* [BMWi07a] thematisiert. Die Ergebnisse der Studie flossen dann in die Vorbereitung der BMWi-Expertenkonferenz *RFID: Towards the Internet of Things*, die im Rahmen der deutschen EU-Ratspräsidentschaft im Jahr 2007 stattfand, ein. Dafür wurde vom Bundeswirtschaftsministerium in Kooperation mit dem Bundesforschungsministerium und der Europäischen Kommission sowie einem Kreis von deutschen und europäischen RFID-Experten das Positionspapier *European Policy Outlook RFID* erarbeitet, das eine Reihe von Empfehlungen für den breiten Roll-out von RFID-Anwendungen und –Diensten enthält [BMWi07b]. Im Positionspapier wurden gezielte Aktivitäten der Europäischen Kommission zur Unterstützung des Aufbaus eines dezentralen und sicheren ONS-Dienstes vorgeschlagen.

Zur Nachfolgekonferenz der französischen Ratspräsidentschaft *Internet of the Future* im Oktober 2008 in Nizza propagierte die französische Regierung die Errichtung eines europäischen ONS-Dienstes. Dazu stellten die französische GS1 France und Orange France, eine Tochter der France Télécom, einen entsprechenden Prototyp eines europäischen ONS-Dienstes vor. Das Bundeswirtschaftsministerium warf zur Nizza-Konferenz in seiner Fortschreibung des *European Policy Outlook RFID* im *Reflection Paper of the Federal Government of Germany* erneut die Frage nach dem freien Zugang zu allen Diensten und dem Schutz vertraulicher Daten im Internet der Dinge auf [BMWi08] (siehe hierzu auch 3.1.1.2).

Ähnliche Bedenken äußerte die Europäische Kommission in ihrem Working paper *Early Challenges regarding the „Internet of Things"*, das sie zur gegenwärtigen Online-Konsultation zu den frühen Herausforderungen des Internet of Things veröffentlicht hat. In dem Papier wird ein weitere Konsultation der Mitgliedsstaaten, der nationalen Datenschutzbehörden und der Wirtschaft vorgeschlagen, um die Minimalanforderungen der nationalen Regierungen an die Transparenz (visibility) und Kontrolle kritischer Komponenten im Internet der Dinge, die für eine Wahrung des öffentlichen Interesses notwendig sind, zu definieren [EC08].

3. Der Stand der ONS-Entwicklung und Perspektiven

Namensdienste für das Internet der Dinge sind ein zentrales Element für den globalen Informationsaustausch im Internet der Dinge. Technisch betrachtet sind Namensdienste verteilte Systeme, die die folgende wichtige Suchfunktion bereitstellen: Bei Eingabe eines Identifikators für einen Gegenstand, z. B. eines Elektronischen Produktcodes (EPC), wird eine Liste von Internetadressen für Dienste zurückgegeben, die weitere Informationen über den Gegenstand anbieten. Solche Dienste können z. B. die Form von EPC Information Services (EPCIS) besitzen, deren Kommunikationsprotokolle ebenfalls von EPCglobal standardisiert werden.

Neben dem EPC-Namensdienst Object Naming Service (ONS) und alternativen Architekturen für diese Grundfunktionalität wird im Augenblick auch an erweiterten Suchdiensten wie den Discovery Services gearbeitet, die eine reichhaltige Semantik zur Auffindung von EPCIS bieten sollen, im Moment aber noch nicht standardisiert sind.[4]

Ohne derartige Namensdienste und Discovery Services, die als Vermittler zwischen Gegenständen und zugehörigen Informationsquellen dienen, könnte das Internet der Dinge nicht den Grad an Flexibilität und globaler Skalierbarkeit erreichen, der zur Erfüllung seiner Vision notwendig ist, die Informationsverarbeitung in komplexen Wertschöpfungs- und Logistikketten in Fertigung und Handel fundamental zu verändern. Durch die vereinfachte Auffindbarkeit objektbezogener Informationen wird eine höhere Transparenz der Wertschöpfungsprozesse ermöglicht.

Die Anwendungsfelder derartiger Namensdienste können in folgende drei Gruppen strukturiert werden:

- Fertigung
- Logistik
- Privates Umfeld

Mit *Fertigung* sind Transformationsprozesse gemeint, die aus natürlichen wie bereits produzierten Ausgangsstoffen lagerbare Wirtschafts- oder Gebrauchsgüter erzeugen. Unter *Logistik* werden Prozesse der Ortsveränderung von Wirtschafts- oder Gebrauchsgütern verstanden. Untersuchungsgegenstand ist hier die gesamte Wertschöpfungskette angefangen beim kleinsten Zulieferer bis hin zum OEM (Original Equipment Manufacturer), der die gelieferten Komponenten zusammenfügt und unter dem eigenen Markennamen verkauft. Unter *Privates Umfeld* sind Zukunftskonzepte wie Intelligentes Haus, Intelligentes Büro, Personalisierte Automatisierte Beratungsdienste (z. B. Ernährungsberatung, Intelligente Hausapotheke) sowie Anwendungen im Gesundheitswesen zusammengefasst.

Die Vorteile von Namensdiensten für diese Anwendungsfelder sind in Tabelle 1 beschrieben.

Tabelle 1: Vorteile von Namensdiensten in verschiedenen Anwendungsfeldern

Anwendungsfeld	Vorteile Namensdienst, z. B. ONS
Fertigung	Effizienzsteigerung in diversen Fertigungsprozessen Vereinfachung globaler Geschäftsbeziehungen Flexibilität bei der Teilnehmerschaft an Wertschöpfungsnetzen
Logistik	Vereinfachung globaler Geschäftsbeziehungen Erleichterung des Informationsaustauschs über Güter in globalen Logistiknetzen Flexibilität bei der Teilnehmerschaft an Wertschöpfungsnetzen Erhöhte Transparenz Effizienzsteigerungen Kostensenkung Rückverfolgbarkeit von Komponenten und Gütern
Privates Umfeld	Einfache Produktidentifikation Rückverfolgbarkeit von Produkten Neue Dienste für intelligente Büro- und Wohnumgebungen Unterstützung von Beratungsdiensten

[4] Siehe [BRI08]

Um diese Vorteile zu gewährleisten, muss ein Namensdienst für das Internet der Dinge wichtige Anforderungen in verschiedenen Kategorien erfüllen, deren Konkretisierung zum Teil abhängig sind von zukünftigen Anwendungsbeispielen, z. B., ob es harte Echtzeitanforderungen für eine Antwort gibt oder nicht. Darum muss auch hier der vorläufige Charakter der Anforderungserhebung im iterativen Entwicklungsprozess beachtet werden.

Tabelle 2: Anforderungen an einen Namensdienst

Kategorie	Unterkategorien (Beispiele)	Weitere Präzisierung (Beispiele)
Funktionalität	Unterstützte Teilnehmer Unterstützte Identifikations-Formate Art der Information Publikationsfunktion Anfragefunktion	EPC: Objektlevel EPC: Individuallevel (Seriennummer)
		Neben Adressdaten auch Daten zum Objekt selbst (z. B. „out-of-service“)?
Skalierbarkeit	Anzahl beteiligter Provider und Server Anzahl Clients Anzahl EPCs und Dokumente	„Niedrig“ ($<10^4$) „Mittel“ (10^5) „Hoch“ ($>10^6$)
Performance	Geschwindigkeit der Antwort Belastung der Server	Antwortzeit < 1 h Antwortzeit < 10 s Antwortzeit < 1 s
Sicherheit	Verfügbarkeit Integrität Vertraulichkeit	Vertraulichkeit der Adressdokumente Vertraulichkeit der Anfrage Anonymität der Clients

Im folgenden Abschnitt diskutieren wir zunächst die genaue Architektur von ONS, des offiziellen Namensdienstes im EPCglobal-Netzwerk. Im Anschluss werden exemplarisch zwei ONS-Alternativen präsentiert (MONS und OIDA), die sich besonders durch ihren Grad an Dezentralität und ihre inhärenten Sicherheitsmechanismen unterscheiden.

3.1 Object Naming Service (ONS)

Der Object Naming Service (ONS) ist der bisher einflussreichste Vorschlag für eine Namensdienstarchitektur für das Internet der Dinge. Der Entwurf des ONS stammt vom Industriekonsortium EPCglobal [EPC08].

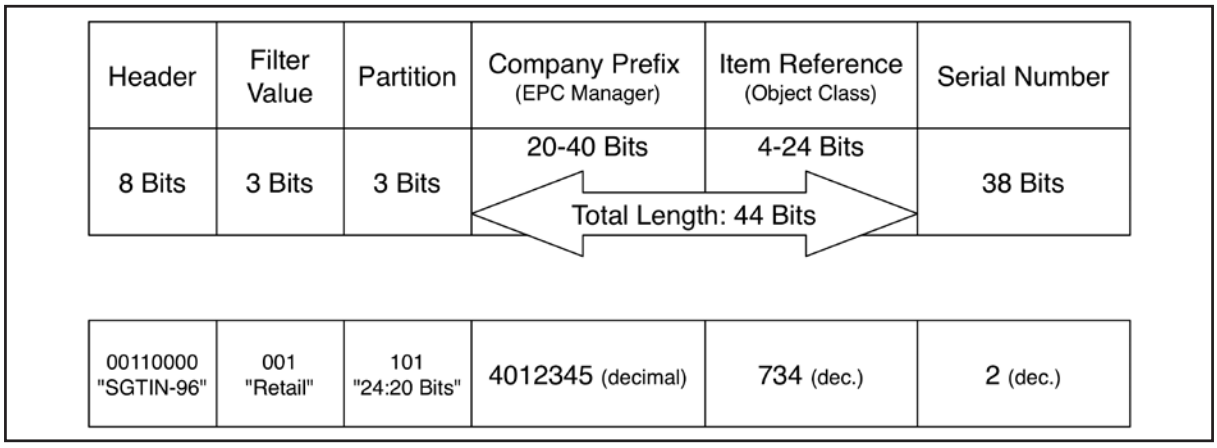
Im Folgenden beschreiben wir Technik und Organisation des ONS sowie damit verbundene Herausforderungen.

3.1.1 Technik und Organisation

Jeder mit dem EPC-Standard konforme RFID-Tag trägt einen EPC, mit dem das Objekt, welches mit dem Tag versehen ist, weltweit eindeutig identifizierbar ist. Somit kann der EPC als eindeutiger Suchschlüssel für die informationstechnische Verfolgung eines Objektes und für den Austausch objektbezogener Informationen dienen. Im EPC-Standard sind verschiedene Namensräume und Kodierungsschemata integriert, so zum Beispiel für „Serialised Global Trade Item Number“ (SGTIN), „Serial Shipping Container Code“ (SSCC) und „Global Returnable / Individual Asset Identification“ (GRAI / GIAI).

Wie bereits angesprochen, ist ein EPC der Variante SGTIN-96, die den Nachfolger des EAN/UCC Barcodes bildet, strukturell in die folgenden Segmente untergliedert (Abbildung 3: EPC-Variante SGTIN-96): „Header“ (Art des EPC, hier SGTIN-96), „Filter Value“ (genereller Objekttyp für Logistik), „Partition“ (Hilfsfeld für variable Länge der beiden folgenden Werte), „Company Prefix“ (auch „EPC Manager“), „Item Reference“ (auch „Object Class“, spezifischer Objekttyp) und „Serial Number“ (Seriennummer, zusammen mit den anderen Segmenten eindeutig). Für ONS sind entsprechend der bisherigen Spezifikation das Company Prefix (EPC Manager) und Item Reference (Object Class) besonders relevant. Die Vergabe eindeutiger Nummern ermöglicht es, objektbezogene Informationen getrennt vom Objekt auf Servern im Internet zu verwalten. Mithilfe des ONS lassen sich die mit einem EPC assoziierten Dienste (EPCIS) auffinden, über die wiederum Informationen zum entsprechenden Objekt abgerufen werden können.

Abbildung 3: EPC-Variante SGTIN-96



3.1.1.1 ONS Architektur

Im EPC-Netzwerk können verschiedene Parteien (Hersteller, Zulieferer, Logistik-Dienstleister, Supermärkte) flexibel in die Infrastruktur des Netzwerkes eingebunden werden.[5] Jede Partei kann Informationen, die sie zu einem bestimmten Objekt gesammelt hat, über Informationsdienste zur Verfügung stellen und diese dynamisch im Netzwerk registrieren. Aufgrund der gegebenen Dynamik in diesem globalen Netzwerk

[5] Siehe [EPC07]

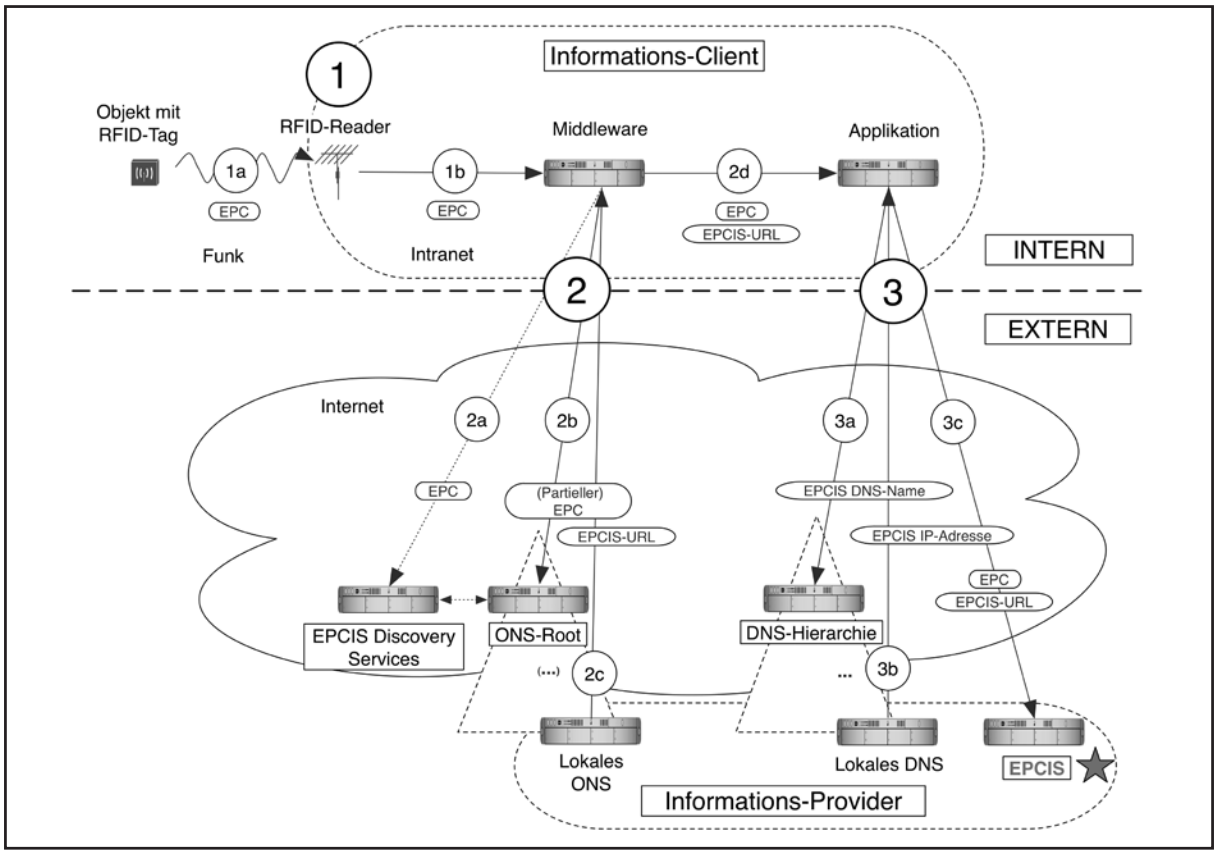
würden statische Listen mit objektbezogenen Datenquellen schnell veraltet sein. Um eine aktuelle Auflistung der relevanten Datenquellen zu erhalten, kann für jede Informationssuche zunächst das ONS befragt werden. Bei Anfragen zu einem EPC gibt das ONS eine aktuelle Liste mit Informationsdiensten für das entsprechende Objekt zurück. In der aktuellen Planung sollen dies allerdings nur Informationsdienste des Herstellers des Objekts sein, was eine organisatorische Einengung der Funktionalität darstellt. Beliebige Informationsquellen sind für die noch nicht fertiggestellten EPC Discovery Services vorgesehen.

Technisch basiert das ONS auf dem Domain Name System (DNS). Die Grundidee besteht darin, einen EPC in einen syntaktisch korrekten Domainnamen zu konvertieren und die existierende Infrastruktur, Software und Protokolle des DNS für die Suche nach weiteren Informationen zu nutzen.[6]

Um Informationsquellen zu einem EPC aufzufinden, werden in der Regel die Adressen (meist in Form von DNS-Namen) von EPCIS für das betreffende Objekt benötig.

Eine Applikation oder eine Middleware verwandelt in einem Zwischenschritt den EPC zunächst in einen URI (Uniform Resource Identifier). Die im ursprünglichen EPC binär codierte SGTIN 47400.11015.473201 (dezimal) wird hierbei in die Zeichenkette „urn:epc:id:sgtin:47400.11015.473201“ umgewandelt. Diese Zeichenkette wird anschließend vom eigentlichen ONS-Resolver in einen Domainnamen umgewandelt (z. B. „47400.11015.sgtin.id.onsepc.com“). Nach der aktuellen ONS-Spezifikation ist der Seriennummernteil des EPC (im Beispiel 473201) nicht in dem korrespondierenden Domainnamen enthalten, jedoch wird explizit Raum für entsprechende künftige Erweiterungen gelassen.

Abbildung 4: Kommunikationsfluss im EPCglobal-Netzwerk



[6] Siehe [EPC08]

Der so erstellte DNS-Name gehört zur Domain onsepc.com, die speziell für ONS reserviert ist. Existiert beim vom Client befragten (meist lokalen) Server kein Eintrag für diesen Namen aus einem früheren Anfrageprozess (Caching), so wird eine neue Anfrage an das ONS-Root gestellt (Schritt 2 in der Abbildung 4), wobei das reguläre DNS-Protokoll verwendet wird. Dabei werden zumindest Teile des angefragten EPC (mindestens Company Prefix und Item Reference) im Klartext über das Internet versendet, da dies inhärent notwendig für die Delegation der Suchanfragen ist. In diesem Schritt sollen auch künftige Discovery Services kontaktiert werden (Schritt 2a).

Das ONS liefert die EPCIS-Adressen des Herstellers zurück, die für den angefragten EPC relevant sind. Diese Adressen liegen in Form von üblichen URLs vor, d. h., sie enthalten ihrerseits DNS-Namen, die wiederum über das klassische DNS in IP-Adressen aufgelöst werden müssen (Schritt 3a), bevor schließlich die eigentlichen EPCIS zum Zwecke des Informationsabrufs kontaktiert werden können (3b).

3.1.1.2 Machtstruktur

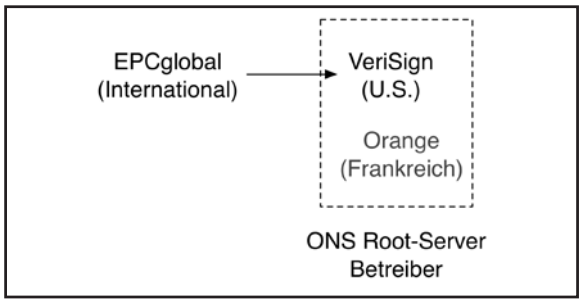
Dieser technische Ablauf – verbunden mit Architekturentscheidungen von EPCglobal – führt zu politisch-organisatorischen und sicherheitsrelevanten Herausforderungen. Der Hauptbetreiber des ONS-Roots, VeriSign, ist ein Unternehmen, das der Gesetzgebung der USA untersteht, was für eine internationale Infrastruktur von derartiger Kritikalität nicht unproblematisch erscheint. Diese einseitig zentrierte Architektur löste eine große Kontroverse aus und führte zur Entwicklung eines unabhängigen ONS-Rootsservers, der vom französischen Unternehmen Orange im Auftrag von GS1 France betrieben wird.

Da kein Abkommen zwischen EPCglobal und GS1 France bezüglich der Interoperabilität der Rootserver existiert, hat GS1 France eine Arbeitsgruppe initiiert, die eine neue ONS-Architektur mit Unterstützung für mehrere unabhängige ONS-Roots entwerfen soll. Diese Arbeitsgruppe besteht aus Mitarbeitern von GS1 France, AFNIC (Registrierungsstelle für die .fr Domain), Afilias (Registrierungsstelle für .info und.aero Domains und Service Provider für die .org Domain), INRIA (Institut national de recherche en informatique et en automatique), dem Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin sowie dem Institut für Pervasive Computing der ETH Zürich. Zurzeit führt diese Gruppe eine Bewertung und Vereinheitlichung von mehreren ONS-Architekturvorschlägen durch. Der endgültige Architekturvorschlag soll von GS1 France als Change Request für den ONS Standard bei EPCglobal eingereicht werden.

Derzeit bleibt noch ungewiss, ob andere Staaten dem Vorbild Frankreichs folgen und eigene ONS-Wurzelknoten betreiben werden, und wie unabhängig diese in der Praxis von VeriSign sein können. Offene Fragen betreffen u. a. die Anzahl, Koordination und den Datenabgleich zwischen den Wurzelknoten und die Verwaltung der ONS-Wurzeldatei sowie die Integrierbarkeit alternativer Architekturen für einzelne Länder oder Regionen.

Das ONS-Root hat die Kontrolle darüber, an welche EPC-Manager die Anfrage weitergeleitet wird. Der EPC-Manager hat die Hoheit darüber, welche EPCIS mit ONS gefunden werden können. Bei der Suche nach beliebigen relevanten EPCIS für ein Objekt (also auch unabhängig vom jeweiligen Hersteller betriebene) sollen die noch nicht spezifizierten EPCIS-Discovery Services eine wichtige Hilfestellung leisten.

Abbildung 5: Machtstruktur beim ONS



3.1.1.3 Ökonomische Aspekte

Tabelle 1 zeigte die Vorteile von ONS und Discovery Services für verschiedene Anwendungsfelder. Es wird ersichtlich, dass Fertigungsunternehmen am wenigsten von diesen Diensten profitieren. Allerdings tragen Fertigungsunternehmen den größten Anteil der Kosten für die Bereitstellung und die Wartung des

EPCglobal Architekturkonzeptes und für den Namensdienst (insbesondere EPCglobal-Gebühren, Bereitstellung von EPCIS und Kosten für RFID Tags.):

Eine solche Unausgewogenheit von Anreizen kann die Entwicklung des Internets der Dinge – in dem nach der EPCglobal-Architektur[7] Namensdienste eine zentrale Rolle spielen – signifikant abbremsen.

Während in Fällen, in denen RFID auch für Produktionsschritte genutzt wird, die Kosten von RFID-Tags vernachlässigt werden können und die EPCIS durch diejenige Partei eingesetzt und unterhalten werden können, die am meisten davon profitiert, muss der Hersteller dennoch die entsprechenden EPC-Nummernbereiche bestellen und bezahlen. Da sie dafür jedoch keinen Anreiz haben, könnten sie möglicherweise diese Kosten zu Parteien mit direkten Anreizen für die Namensdienstleistungen transferieren, was in signifikanten Kosten für diese Parteien resultieren könnte.

3.1.2 Sicherheit

Das DNS ist ein klassischer und zentraler Internetdienst mit einer langen Geschichte von Sicherheitsproblemen, sowohl im eigentlichen Protokoll als auch in seinen konkreten Implementierungen. Viele Schwachstellen des DNS sind dadurch bedingt, dass der Dienst, der jederzeit allgemein zugänglich sein muss und für zahllose Anwendungen benutzt wird, keinerlei Authentifizierungsmechanismen beinhaltet. Über das DNS-Protokoll können weder der jeweils befragte Server noch die erhaltenen Informationen authentifiziert werden, zudem verläuft die gesamte Kommunikation im Klartext. Da das ONS auf dem DNS basiert, übertragen sich diese Schwachstellen direkt auf das ONS.[8]

3.1.2.1 Integrität

Ein wichtiges Problem stellt die Integrität der Informationen aus dem ONS dar. Dies bezieht sich auf die Korrektheit und Vollständigkeit der über das ONS erhaltenen Daten. Mithilfe von regulär oder durch Systemeinbruch kontrollierten ONS-Servern oder Man-in-the-Middle-Angriffen auf die Kommunikation könnten Angreifer gefälschte Daten in die Anfrageresultate einschleusen. Beispielsweise könnten Adressen von EPCIS, die unter der Kontrolle eines Angreifers stehen, in die Liste eingebracht werden. Sofern dies nicht durch Authentifizierungsmechanismen verhindert wird, könnten Angreifer gefälschte Informationen zu dem angefragten Objekt bzw. zu vielen weiteren Objekten aus dieser Domäne liefern.

Setzt sich das EPC-Netzwerk auf breiter Basis durch, so ist zu erwarten, dass eine wachsende Zahl von Anwendungen auf seine Dienste zurückgreift. Dies gilt sowohl für Anwendungen in den Bereichen B2B und B2C als auch im privaten Umfeld. Insbesondere ist beabsichtigt, das ONS in zentrale Geschäftsprozesse zu integrieren. Solche Anwendungen wären auf zuverlässige Lösungen zum Auffinden objektbezogener Datenquellen dringend angewiesen. ONS benutzt das etablierte DNS- (Domain Name System) Protokoll des Internets, bei dem alle Nachrichten im Klartext und meist auf Basis des zustandslosen User Datagram Protocol (UDP) versendet werden, das aus Geschwindigkeitsgründen keine Fehlererkennung oder Sequenznummern für Nachrichten benutzt.

Die dem DNS-Protokoll eigenen Identifikationsnummern zur Zuordnung von Anfrage und Antwort sind ungeeignet, um in der Praxis zu verhindern, dass die Kommunikation oder sogar in bestimmten Fällen die DNS-Daten auf den Servern selbst von Dritten gefälscht werden kann. Im Sommer 2008 ist dieses Problem auch in den Massenmedien bekannt geworden.[9] Hintergrund sind fundamentale Lücken in der DNS-Datenauthentifizierung und in vielen etablierten DNS-Servern.[10]

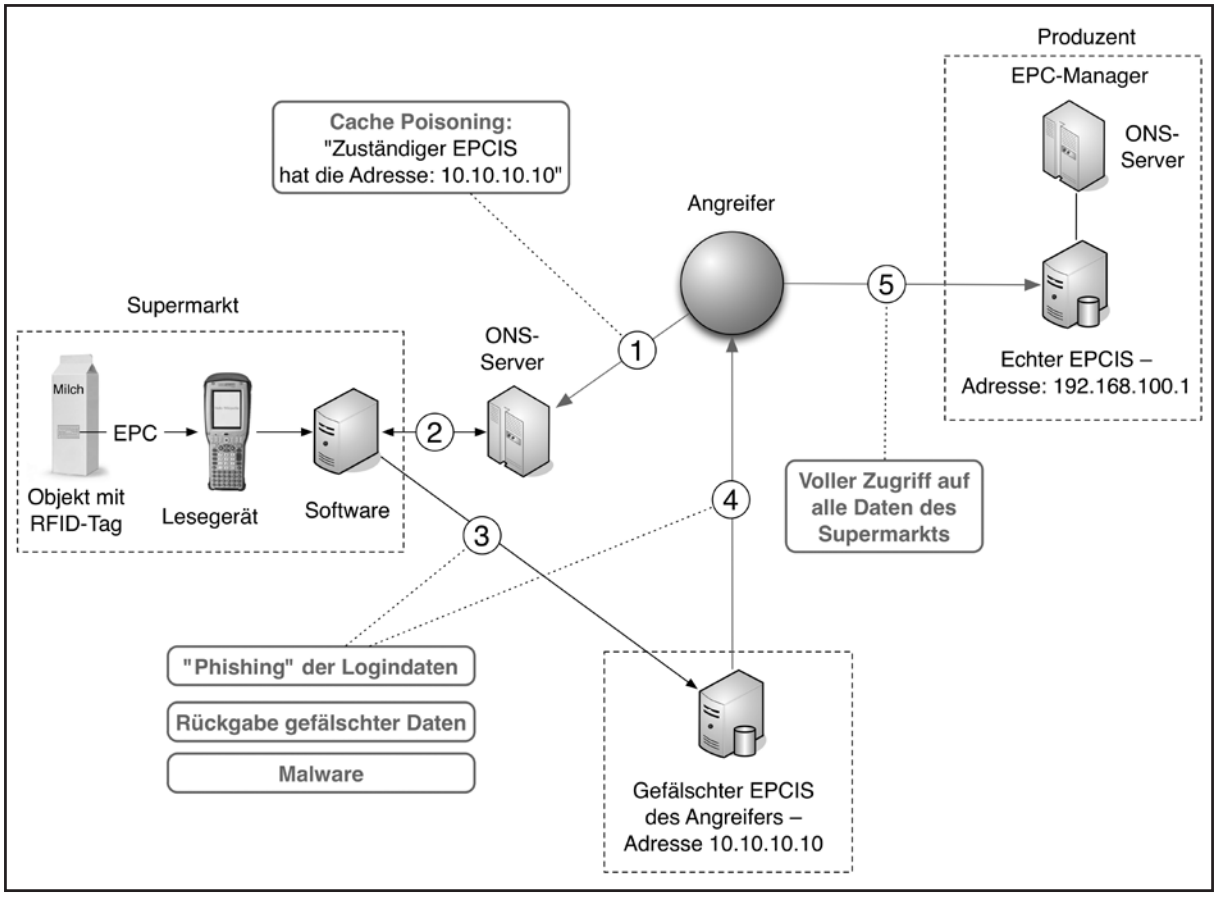
7 Siehe [EPC07]

8 Siehe [FGS05], [FG09]

9 z. B. Spiegel-Online vom 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 Siehe US-CERT http://www.kb.cert.org/vuls/id/800113 und die Homepage von DNS-Forscher Dan Kaminsky: http://www.doxpara.com/?p=1162 (10/2008).

Abbildung 6: Ablauf eines „Cache Poisoning“-Angriffs



Solche etablierten Angriffsmuster, z. B. Man-in-the-Middle-Angriffe oder Cache Poisoning, können einfach auf das ONS übertragen werden, da Software und Protokolle direkt auf dem DNS basieren. In der jetzigen ONS-Spezifikation gibt es keine Möglichkeit zur Gewährleistung von Integrität und Authentizität der Adressdaten.

Ein Mangel an Integrität der Daten im ONS kann dazu führen, dass ein Angreifer systematisch Suchanfragen an beliebige Ziele umleiten kann, so z. B. an EPCIS-Server unter seiner eigenen Kontrolle. Der Ablauf eines solchen „Cache Poisoning“-Angriffs sei kurz skizziert (Abbildung 6):

1. Ein Angreifer manipuliert die Adresseinträge auf einem beliebigen ONS-Server, z. B. mit der Information, dass der EPCIS für ein Produkt unter einer anderen IP-Adresse zu erreichen sei (10.10.10.10 statt korrekt 192.168.100.1 im Beispiel). Hierzu gibt es etablierte Angriffsprogramme, die verschiedene Schwachstellen der DNS-Server-Programme und des Protokolls ausnutzen können.[11]

2. Zu einem späteren Zeitpunkt befragt ein regulärer Client den ONS-Server in der Erwartung einer korrekten Antwort. Stattdessen wird die manipulierte Adressinformation (10.10.10.10) vom Server zurückgegeben, ohne dass der Client dies bemerken kann.

3. Der Client verbindet sich nun zum EPCIS bei 10.10.10.10. Hieraus können sich vielfältige Folgerisiken ergeben:

[11] Zum Beispiel als Plugin für das etablierte Metasploit-Framework: http://www.metasploit.com/.

Im einfachsten Falle erhält der Client keine der benötigten Informationen zum angefragten EPC, was dazu führen kann, das die betreffende Anwendung nicht korrekt arbeiten kann (Denial of Service).

Der gefälschte EPCIS kann als Webservice versuchen, die Clientsoftware mit sogenannter „Malware" zu infizieren (Viren, Backdoors, Bot-Software), so wie bereits oft beim klassischen Web-Surfen Sicherheitslücken im Browser (d. h., dem Webclient) von bösartigen Servern ausgenutzt werden.

Schließlich kann der Angreifer versuchen, seinen EPCIS als korrekt auszugeben. Dies kann gelingen, wenn z. B. weitergehende Sicherungsmaßnahmen bei der EPCIS-Verbindung nicht vorhanden sind oder ignoriert werden (z. B. Warnungen bei gefälschten SSL-Zertifikaten). In diesem Fall kann der Angreifer beliebige gefälschte Produktinformationen an den Client zurückgeben, die dort in die Geschäftsprozesse einfließen werden. Weiterhin kann der EPCIS die korrekten Login-Daten des Clients abfangen und sich selbst Zugang beim korrekten EPCIS und den dort vorhandenen Daten verschaffen (siehe Schritte (4) und (5) in der Abbildung).

Aus dem Mangel an Maßnahmen zur Integrität und Authentizität im ONS können sich somit vielfältige indirekte Risiken ergeben, je nach Anwendungsfeld und Ausgestaltung zusätzlicher Schutzmaßnahmen:

Tabelle 3: Risiken durch Mangel an Integritätsschutz

Anwendungsfeld	Indirekte Risiken durch Mangel an Integrität und Authentizität im ONS
Fertigung	Einschränkung der Funktionalität Fertigungsstillstand Sabotage Wirtschaftsspionage
Logistik	Einschränkung der Funktionalität Fälschung von Objektdaten Manipulation von Prozessen Datenverlust Wirtschaftsspionage
Privates Umfeld	Fälschung von Produktdaten Eingeschränkte oder falsche Funktionalität der Dienste für intelligente Büro- und Wohnumgebungen Eingeschränkte oder falsche Funktionalität der Beratungsdiensten Spam

Bei der Absicherung des ONS ist ferner zu beachten, dass die dort gespeicherten Adressdaten wiederum DNS-Namen für Server benutzen. Um das ONS also umfassen zu sichern, müssten auch die benutzten DNS-Einträge durch Authentifizierungsmaßnahmen wie DNSSEC (siehe unten Abschnitt 3.4) geschützt werden.

3.1.2.2 Verfügbarkeit

Das ONS wird zu einem hohen Maße möglichen Angriffen aus dem Internet ausgesetzt sein, da es notwendigerweise einer großen Anwenderzahl zugänglich ist. Besonders das relativ zentrale, auf nur wenige Server verteilte ONS-Root stellt einen „Single Point of Failure“ dar. Daraus ergeben sich Risiken wie Distributed-Denial-of-Service (DDoS) Angriffe, siehe Abbildung 7. Bei solchen Angriffen werden einzelne Server oder deren Internetverbindung durch eine hohe Zahl künstlich erzeugter, paralleler Anfragen überlastet, die von sehr vielen sogenannten „Bots“ durchgeführt werden, d. h. durch Malware infizierte normale Computer ohne Wissen ihrer Besitzer oder regulären Benutzer.

Alternativ können spezielle Softwarefehler von Angreifern ausgenutzt werden, um mittels Angriffsprogrammen (sogenannten „Exploits“, Programmen zur Ausnutzung von Sicherheitsschwachstellen) den angegriffenen Dienst zu deaktivieren oder aus der Ferne zu übernehmen.

Eine spezielle Form von Angriffen auf die Verfügbarkeit wäre durch die Kontrolle des ONS-Roots oder aller zu ihm führenden Netzwerkverbindungen möglich. Bei dieser sogenannten Root-Blockade könnten selektiv Anfragen aus bestimmten Ländern, oder sogar von bestimmten Clients blockiert werden, während andere regulär beantwortet würden. Dies könnte zu einer virtuellen Embargo-Situation führen, bei der ein Land systematisch von der Nutzung des ONS ausgeschlossen wird. Wenn die Nutzung des Internets der Dinge zunimmt und seine Suchfunktionalität in wichtigen Geschäftsprozessen genutzt wird, so könnte eine Root-Blockade einen effektiven Angriff auf eine kritische Infrastruktur eines Staates darstellen.

Abbildung 7: Ablauf eines verteilten „Denial of Service“-Angriffs

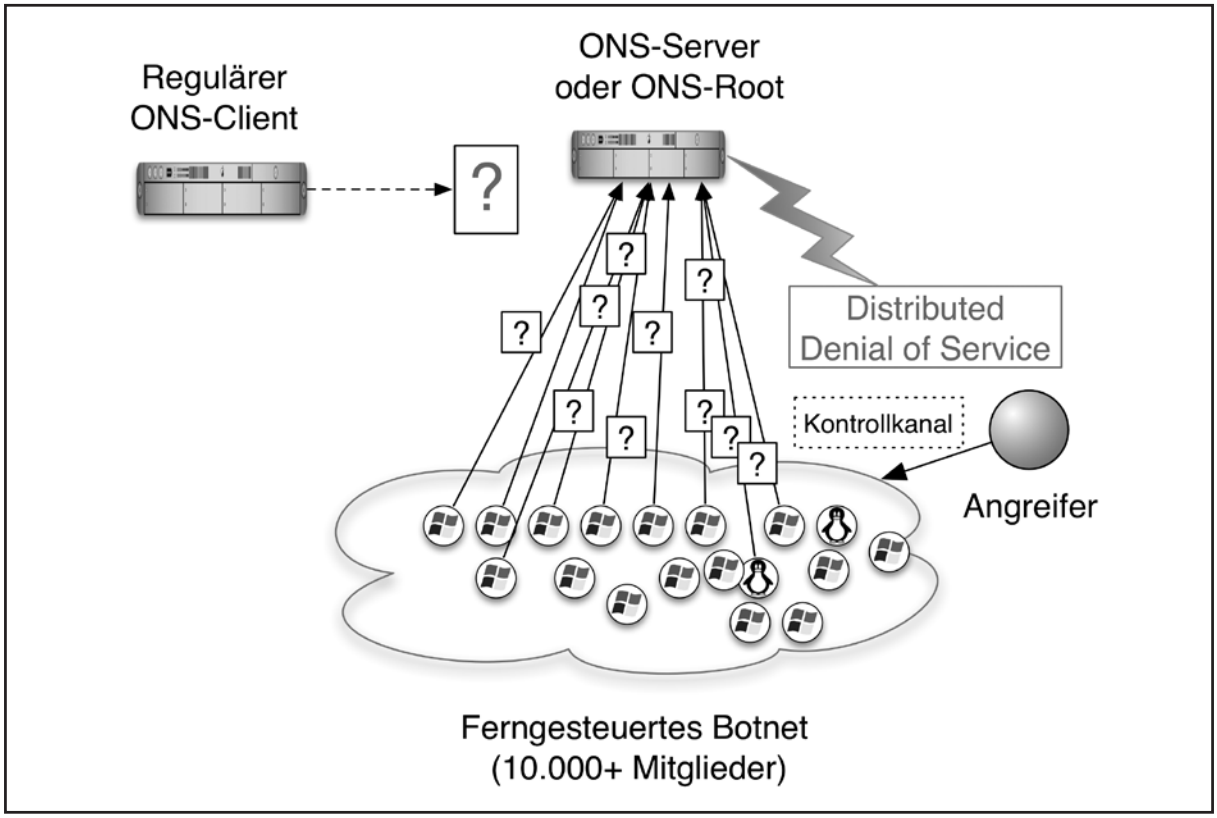


Tabelle 4: Risiken durch Mangel an Verfügbarkeitsschutz

Anwendungsfeld	Risiken durch Mangel an Verfügbarkeit
Fertigung	Einschränkung der Funktionalität Produktionsstillstand Sabotage
Logistik	Bestell- und Lieferprobleme Verhinderung von Status-Updates Einschränkung der Funktionalität Sabotage Reduzierte Transparenz
Privates Umfeld	Nicht verfügbare Produktdaten Eingeschränkte Funktionalität von Diensten für intelligente Büro- und Wohnumgebungen Eingeschränkte Funktionalität von personalisierten Beratungsdiensten

3.1.2.3 Vertraulichkeit und Anonymität

In vielen Kontexten könnten die EPCs auf RFID-Tags sowie die zugehörigen Abfragemuster an das Internet der Dinge als sensible Information eingestuft werden, insbesondere wenn sie unbemerkt ohne großen Aufwand gesammelt und systematisch mithilfe von Data-Mining-Verfahren ausgewertet werden können.[12] Beispielsweise kann die Analyse von Waren- und Materialflüssen wertvolle Informationen über Konkurrenten bieten und Preisverhandlungen beeinflussen. Auch personenbezogene Daten lassen sich relativ leicht mit einem EPC verknüpfen, was Lokalisierung und Profiling von Individuen ermöglichen kann.

Selbst wenn der Seriennummernteil des EPC über das Netz nicht bekannt wird, kann bereits aus der Kombination Company Prefix (Hersteller) und Item Reference (Objektklasse) geschlossen werden, zu welcher Art von Objekt der EPC gehört. Cluster von partiellen EPCs können stellvertretend für einen vollständigen EPC zum eindeutigen Schlüssel werden, um Objekte mit Personen oder Unternehmen in Verbindung zu bringen. Auch die Interaktion mit den eigentlichen EPCIS kann aufschlussreiche Rückschlüsse auf das Objekt erlauben.

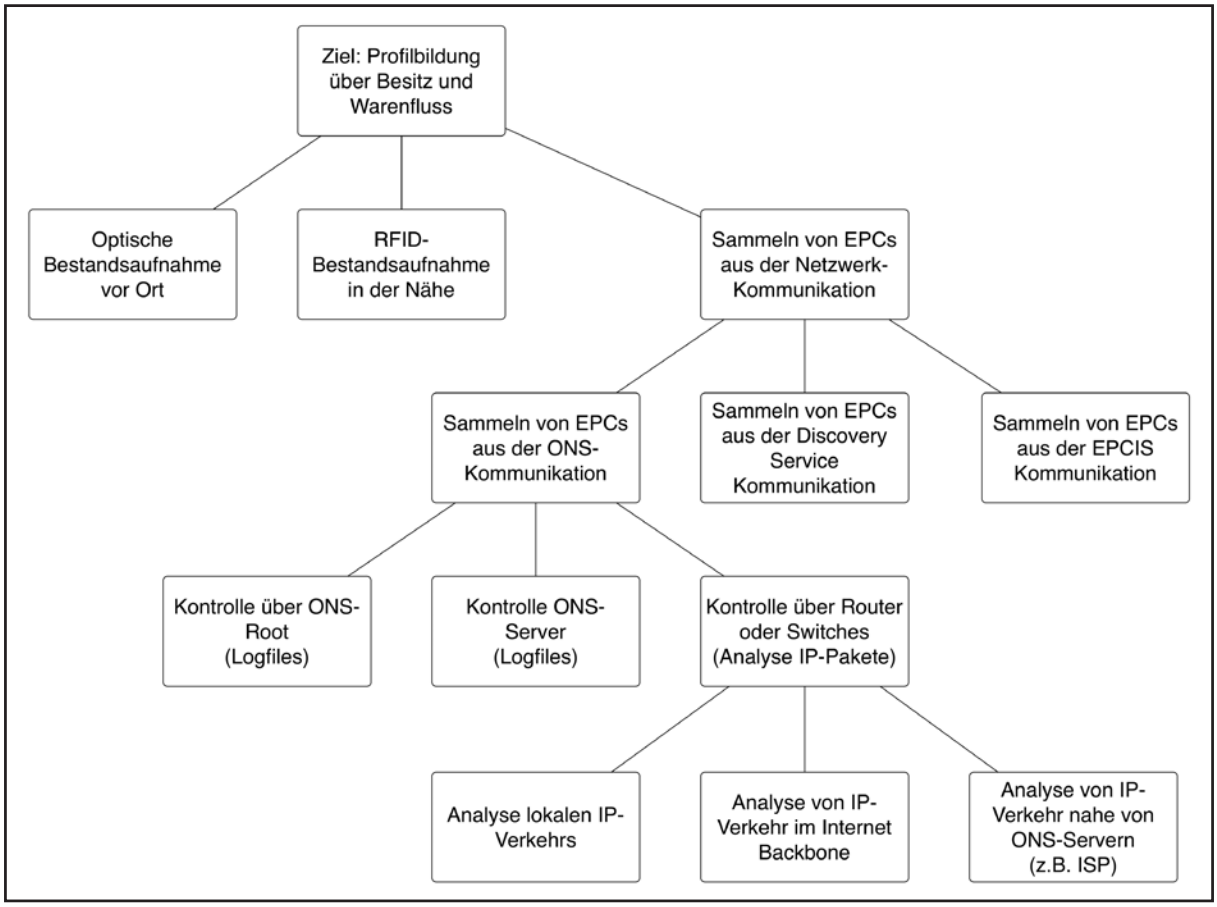
Um potenziellem Missbrauch vorzubeugen, wurden bereits zahlreiche Vorschläge unterbreitet. Im Vordergrund stehen bisher Verfahren, die den EPC auf dem Tag vor unbefugtem Auslesen schützen. Die Kommunikationsprozesse hingegen, die wie die Nutzung des EPC-Netzwerks erst nach dem eigentlichen RFID-Auslesevorgang erfolgen, fanden bisher nur wenig Beachtung.[13]

Um die zu einem EPC gehörigen Informationen aus dem EPC-Netzwerk abzurufen, müssen zunächst die entsprechenden EPCIS über das ONS ausfindig gemacht werden. Am Anfang des Prozesses steht also immer dann, wenn die gesuchte Adresse nicht zufällig bereits in einem temporären lokalen Cache vorhanden ist, die unverschlüsselte Kommunikation mit dem ONS, auch wenn im Anschluss die Verbindung zur eigentlichen Datenquelle (EPCIS) verschlüsselt aufgebaut werden sollte (z. B. mittels SSL/TLS). Der Hauptteil des EPC wird somit für das DNS kodiert und im Klartext zu einem DNS-Server gesendet. Dabei passieren die Informationen das lokale Netzwerk, das gegebenenfalls auch durch ein WLAN realisiert sein kann, was bei fehlenden Sicherheitsmaßnahmen den Netzwerkverkehr leicht abhörbar macht. In Abhängigkeit vom Cache und der Konfiguration des konsultierten DNS-Servers wird die Anfrage entlang des Pfa-

12 Siehe [GS05]
13 Siehe [FG09]

des zur Namensauflösung im DNS weitergeleitet. Dies beinhaltet möglicherweise eine Weiterleitung an einen Root-DNS-Server, ferner an den zuständigen Server für onsepc.com bei VeriSign und eventuell weitere Server aus der DNS- oder ONS-Hierarchie bis hin zu der Firma, die als Hauptreferenz für den angefragten EPC agiert.

Abbildung 8: Strategien zur Profilbildung über Warenflüsse



Alle Internet-Service-Provider, über deren Netze derartige Anfragen weitergeleitet werden, können Teile der angefragten EPCs mithören. Gleiches gilt für Behörden der Länder, über welche die Daten weitergeleitet werden. Daraus ergeben sich neue Möglichkeiten für Angreifer, die aus einer Analyse des EPC-relevanten Datenverkehrs Nutzen ziehen wollen (Abbildung 8).

Auf Basis des DNS-Protokolls ist keine Gewährleistung von Vertraulichkeit der ONS-Daten möglich. So können Anfragen von Nutzern an das ONS einfach von allen Servern, dem ONS-Root oder auch jedem Internet-Service-Provider mitgelesen und samt Ursprungsadresse, die oft personenbeziehbar ist, mitprotokolliert werden. Jede ONS-Anfrage von Firmen oder Personen betrifft Objekte der realen Welt und könnte zur Identifizierung, Profilbildung (Besitz, Beziehungen) und eventuellen groben Ortung der Nutzer eingesetzt werden – analog zu RFID-Datenschutzproblemen, wahrscheinlich weniger granular als durch RFID-Lesegeräte, dafür aber im globalen Maßstab bei großen Nutzergruppen. Dies betrifft auch Firmen, deren Logistik und Beschaffungsstrategien für Dritte transparent werden könnten.

Tabelle 5: Risiken durch Mangel an Vertraulichkeitsschutz

Anwendungsfeld	Risiken durch Mangel an Vertraulichkeit
Fertigung	Wirtschaftsspionage Ausspähung von Güterflüssen Ausspähung von Geschäftsbeziehungen
Logistik	Wirtschaftsspionage Ausspähung von Güterflüssen Ausspähung von Geschäftsbeziehungen
Intelligentes Haus	Profilierung von Privateigentum, Konsumverhalten, Lebensstil, ev. auch von sozialen Kontakten und Bewegungsmustern Indirekte Ausspähung sensitiver Daten (z. B. Krankheiten von Einwohnern aufgrund von ONS-Abfragen zu Medikamenten)

3.1.3 Relevanz von ONS-Geschäftsmodellen

In dieser Studie werden hauptsächlich Sicherheitsaspekte betrachtet, die sich aus dem heutigen Stand der Organisation und technischen Architektur von ONS ergeben. Die möglichen Geschäftsmodelle, die hinter den technischen Implementierungen stehen, werden den korrekten Betrieb und die Sicherheit des ONS sowie der anderen Komponenten der EPCglobal-Architektur ebenfalls stark beeinflussen. In dieser Hinsicht werden auch die folgenden organisatorischen Aspekte relevant sein:

- Regeln für Delegation und Zuteilung von EPCs
- Verfahren und Instanzen zur Last-Ressort Dispute Resolution
- Delegation von Registrierungsdiensten
- Betriebssicherheit der Registratur und Validierung
- Anforderungen an und Akkreditierung von Registrierungsdienstleistern.

3.2 Multipolares ONS

Hier stellen wir Modifikationen der aktuellen ONS-Architektur vor (Multipolares ONS, MONS), welche es erlauben, die Kontrolle über den ONS-Root zwischen verschiedenen unabhängigen Teilnehmern zu verteilen und damit das Problem der einseitigen Kontrolle über den Root zu lösen.[14]

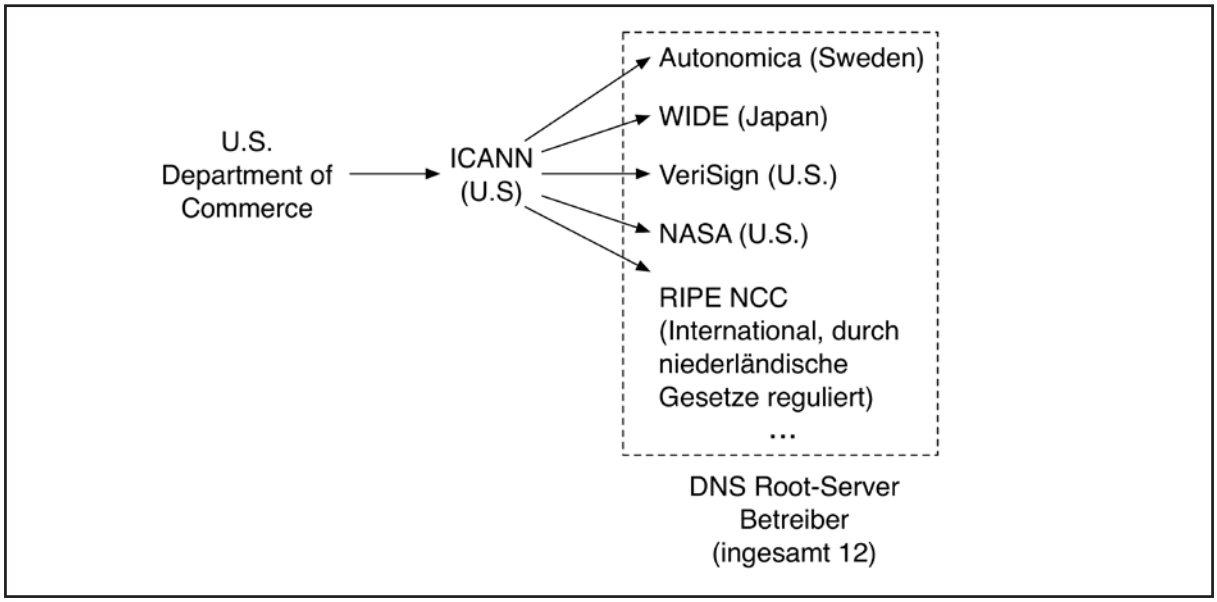
3.2.1 Technik und Organisation

Bevor Modifikationen vorgeschlagen werden, die das Unipolaritätsproblem der bestehenden ONS-Architektur lösen sollen, sollte die folgende Frage beantwortet werden: Wie schwerwiegend ist das Unipolaritätsproblem beim ursprünglichen DNS?

Das DNS stellt aus technischer Perspektive eine Hierarchie von DNS-Nameservern dar, wobei jeder dafür verantwortlich ist, die Hostnamen (z. B. von Webseiten), welche zu seiner Domain gehören, in IP-Adressen aufzulösen oder sie einem anderen DNS-Nameserver zuzuweisen, wenn eine Delegierung stattfindet.[15] Die für Top-Level Domains (TLDs, z. B. .eu, .com) autoritativen DNS-Nameserver werden von speziellen Registrierungsbehörden betrieben – Organisationen, welche für die Verwaltung und den technischen Betrieb der TLDs verantwortlich sind. Die Root-Nameserver werden von staatlichen Behörden, kommerziellen und auch gemeinnützigen Organisationen betrieben. Die Root-Zone wird von dem gemeinnützigen US-Unternehmen „Internet Corporation for Assigned Names and Numbers“ (ICANN) betreut. Zu diesem Zweck wurde die ICANN vom „U.S. Department of Commerce“ vertraglich verpflichtet, wodurch dieses US-Ministerium rechtlich gesehen die Kontrolle über den Root-Namensraum besitzt.

Momentan wird die Root-Zone von nur 13 logischen Root-Nameservern bedient, deren Anzahl aufgrund von technischen Einschränkungen nicht ohne Umstände erhöht werden kann. Tatsächlich jedoch wurden viele dieser Server in vielen anderen Regionen gespiegelt und sind via Anycast[16] erreichbar. Als Folge davon ist gegenwärtig die Mehrzahl der physischen Root-Nameserver außerhalb der USA aufgestellt.

Abbildung 9: Machtstruktur beim DNS



[14] Siehe [EFG08].

[15] Siehe [LA06].

[16] Anycast ist ein Protokoll für die „one-to-many“-Korrespondenz zwischen einer IP-Adresse und mehreren, physisch verteilten Servern, sodass für jede Abfrage ein optimaler, d. h. meist möglichst naher Server gewählt wird (siehe RFC 3258).

Dennoch ist eine solche Konzentration der rechtlichen Kontrolle über den DNS-Root-Namensraum auf eine einzelne Regierungseinrichtung Gegenstand andauernder Kritik der Internetgemeinde. Theoretisch hat diese Einrichtung die Macht, Änderungen an der Root-Zonendatei vorzunehmen. Da die Root-Zone aber faktisch verteilt und gespiegelt wird, müssen solche Änderungen zu allen anderen Root-Nameservern propagiert werden, von denen sich viele jenseits des Einflussbereichs der US-Einrichtung, welche die Root-Zone kontrolliert, befinden. Für den Fall, dass sich diese Regierung entscheidet, ihre Macht zu missbrauchen und Änderungen an der Root-Zone vorzunehmen, um so einzig eigenen Vorteilen zu dienen, könnten sich einige der Root-Nameserver weigern, die Änderungen an ihren eigenen Root-Zonendateien vorzunehmen. Das könnte letztlich zu einer unkontrollierten und permanenten Zerstückelung des zentralen Namenssystems des Internets führen und fundamentale Grundprinzipien des Internets unterlaufen, was Geschäftsrisiken weltweit erhöhen würde.

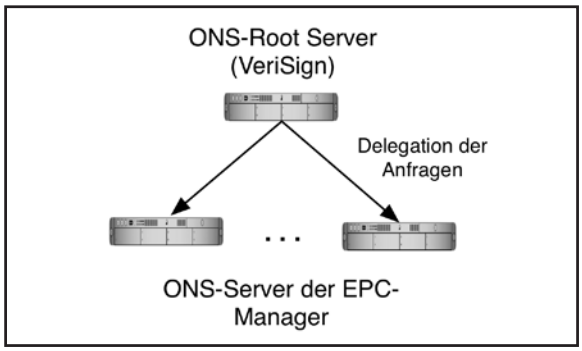
Diese Konsequenzen, ebenso wie die Tatsache, dass solche Änderungen bis jetzt noch nicht aufgetreten sind, erlauben es anzunehmen, dass das Internet faktisch nicht allzu abhängig von der Einrichtung ist, die den Root-Namensraum verwaltet, und es höchst unwahrscheinlich ist, dass diese Einrichtung eigenmächtig Änderungen einführt, die einen fairen und weltweiten Internetzugriff erschweren würden. Folglich ist eine Root-Blockade ohne schwer zu kalkulierende Risiken für das auslösende Land beim DNS nicht realistisch - im Gegensatz zum ONS, bei dem derartige Störungen durchaus denkbar erscheinen, nicht zuletzt im Falle militärischer Auseinandersetzungen.

In folgenden Abschnitten beschreiben wir einen Vorschlag zur Modifikation der momentanen ONS-Architektur. Ziel ist es, die Kontrolle über den ONS-Root unter mehreren, voneinander unabhängigen Teilnehmer zu verteilen und damit das Problem der einseitigen Kontrolle über die Wurzel (Root) zu lösen.

3.2.1.1 Repliziertes MONS

Einer der Hauptgründe, warum DNS für die Umsetzung des Namensdienstes für das EPCglobal Netzwerk ausgewählt wurde, ist eine Verminderung des Aufwands, um ONS im globalen Rahmen einzuführen. Das DNS wird von vielen Fachleuten als eine im Prinzip ausgereifte und bewährte Architektur betrachtet. Seine Wahl erlaubt es, das ONS mit bestehender DNS-Software zu entwickeln und stützt sich auf Erfolgskonzepte langjähriger DNS-Nutzung. Demzufolge kann ein Systemadministrator mit Erfahrung im Umgang mit DNS relativ leicht den Betrieb eines lokalen ONS-Nameservers mit frei verfügbarer Software umsetzen. Wenn wir also die bestehende ONS-Architektur modifizieren wollen, kann es sinnvoll sein, kompatibel zum DNS-Protokoll zu bleiben.

Abbildung 10: Aktuelle ONS-Hierarchie



Der ONS-Root sollte nach ursprünglicher Planung auf sechs global verteilten Serverkonstellationen implementiert werden, die alle von VeriSign betrieben werden (Abbildung 10). Dies steht im starken Kontrast zu der DNS-Architektur, bei der die Root-Nameserver von einer Vielzahl anderer Institutionen betrieben werden. Ein möglicher Ansatz zur Vermeidung der Unipolarität des ONS ist es, den ONS-Root auf einer Vielzahl von Servern nachzubilden, welche durch unabhängige Institutionen betrieben werden und die Instanzen der Root-Zonendatei mit einer Originalkopie, die von EPCglobal veröffentlicht wird, zu synchronisieren. Um die Anzahl der eingehenden Abfragen zu begrenzen, könnte jeder Root-Nameserver dahingehend konfiguriert werden, einen bestimmten Bereich der IP-Topologie abzudecken und nur auf die Abfragen zu antworten, die von dort stammen.

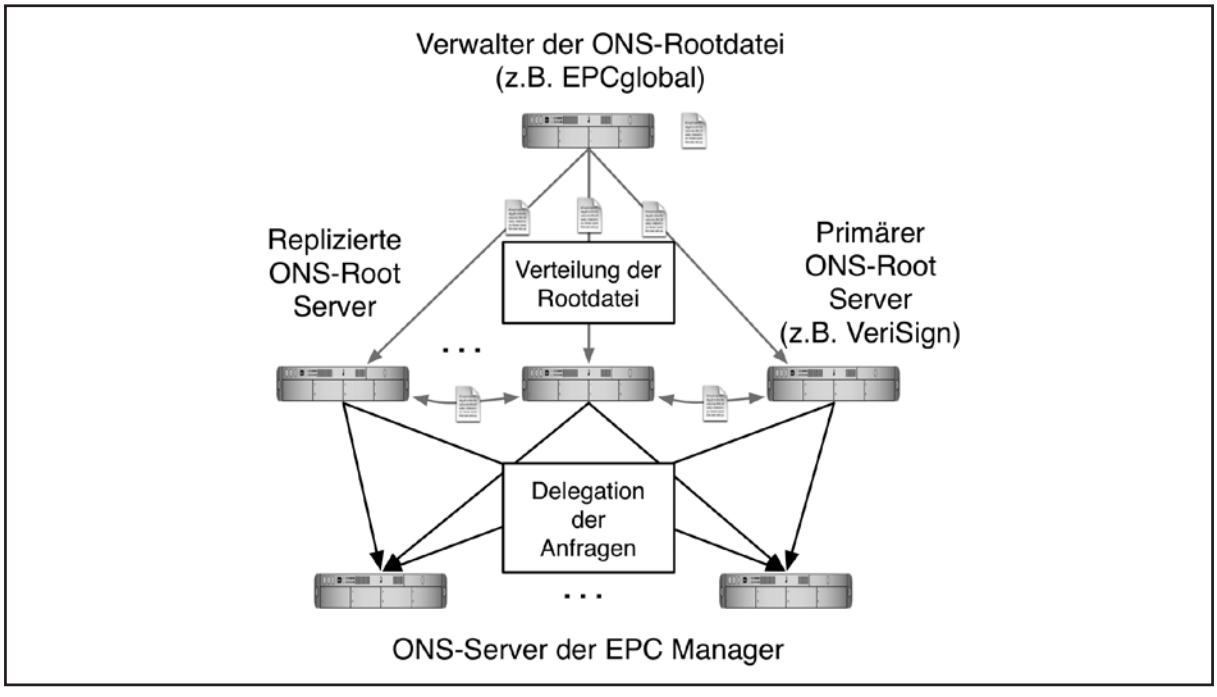
Solche gespiegelten ONS-Root-Nameserver könnten ihre Dienste parallel zum globalen, von VeriSign betriebenen ONS-Root anbieten.[17] Die für die Auflösung von Clientanfragen zuständigen ONS-Server von Unternehmen und Internetdienstanbietern sollten zum einen mit dem Domainnamen oder der IP-Adresse des globalen ONS-Roots (onsepc.com) oder, was deutlich effizienter wäre, mit dem für SGTIN verantwortlichen Server (sgtin.id.onsepc.com) konfiguriert werden, zum anderen auch mit dem korrespondierenden, gespiegelten ONS-Server (z. B. sgtin.id.onsepc-repliocation.eu), um umständliche Anycast-Konstruktionen, wie sie nachträglich für das DNS gebraucht wurden, zu vermeiden.

Um die Durchführbarkeit dieses Ansatzes und die Menge an Daten, welche repliziert werden müssen, zu evaluieren, berechnen wir näherungsweise die Größe der ONS-Root-Zonendatei durch das Schätzen der Anzahl von Einträgen (Resource Records, RRs), die dort gespeichert sind und welche die Abbildungen zwischen Company Prefix und dem Domainnamen der korrespondierenden ONS-Nameserver definieren. Heutzutage gibt es bereits über eine Million registrierter Company Prefixes.[18] Wir nehmen an, dass zu einem bestimmten Zeitpunkt in Zukunft die meisten von ihnen zugehörige EPCIS besitzen. Die ONS-Root-Zonendatei ist eine Klartext-Datei, die aus einer Anzahl von NS RRs (Name Server RRs) besteht. Als ein Beispiel betrachte man eine EPC-Nummer 400453.1734.108265, die in einen von zwei ONS-Nameservern aufgelöst werden kann, um die Anfrage dorthin zu delegieren:

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

IN steht für „Internet“ und „NS“ gibt an, dass der Record einen für die Domain autoritativen Nameserver definiert. Die Anzahl der für die gleiche Zone verantwortlichen Nameserver kann nicht dreizehn überschreiten; die DNS-Spezifikation empfiehlt mindestens zwei im Einsatz.

Abbildung 11: Replikation des ONS-Roots



[17] Eine ähnliche Alternative existierte bis vor kurzem für das DNS-Root: Das unabhängige, von Enthusiasten betriebene Open Root Server Network musste Ende 2008 den Betrieb einstellen (http://european.ch.orsn.net/), siehe auch Heise Netze (23.10.2008): http://www.heise.de/netze/Alternative-DNS-Root-Server-vor-der-Abschaltung--/news/meldung/117863.

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

In der Praxis variiert die Anzahl jedoch zwischen zwei und fünf. Wir nehmen an, die durchschnittliche Anzahl von ONS-Nameservern pro Unternehmen (N) ist vier, die Durchschnittslänge eines NS-Records (L) beträgt 60 Zeichen, wovon ein Zeichen ein Byte benötigt. Die Anzahl der registrierten Company Prefixes (P) liege, wie oben begründet, bei einer Million. Dann können wir die Größe der ONS-Root-Zonendatei, die die RRs für alle momentan registrierten EAN.UCC Company Prefixes enthält, grob mit N x L x P schätzen, womit man bei etwas über 200 Megabyte wäre.

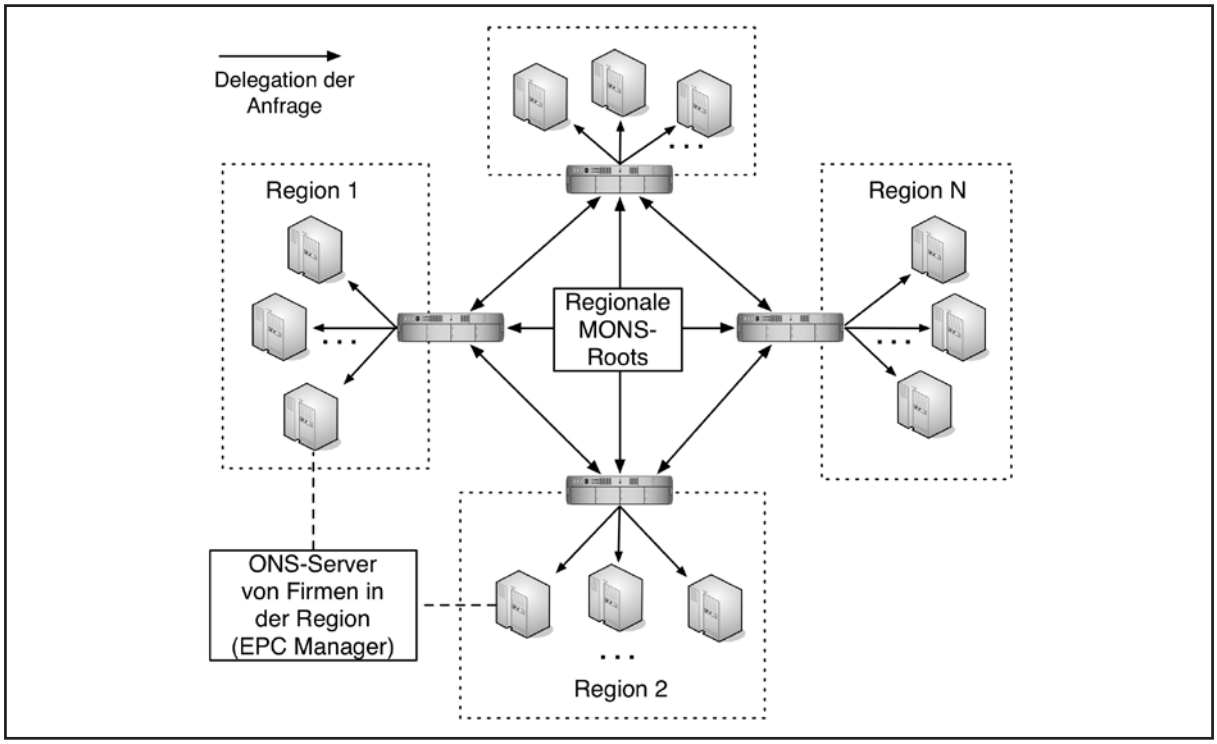
Durch Komprimierung kann eine Textdatei auf 10 bis 20% ihrer ursprünglichen Größe reduziert werden. Also schließen wir daraus, dass die Verteilung und eine regelmäßige Erneuerung der Root-Zonendatei keine technischen Schwierigkeiten darstellen. Die ursprüngliche Root-Zonendatei kann zwischen den ONS-Roots durch eine einfache Datenübertragung oder ein speziell abgesichertes Peer-to-Peer-Filesharing-Protokoll ausgetauscht werden. Die Architektur ist in Abbildung 11 veranschaulicht. Auf sie wird im Folgenden als „Replicated MONS“ (Repliziertes MONS) Bezug genommen.

Eine wichtige Voraussetzung für Replicated MONS ist die öffentliche Verfügbarkeit der ONS-Root-datei. Sobald die Root-Zonendatei veröffentlicht und regelmäßig aktualisiert wird, können die nachgebildeten Roots unabhängig voneinander implementiert werden. Für den Fall, dass diese neuen Roots so konfiguriert werden, dass sie nur bestimmte Bereiche abdecken, sind Standorte außerhalb dieser Abdeckung immer noch in der Lage, die Nameserver von VeriSign zu benutzen, bleiben jedoch durch eine mögliche Root-Blockade gefährdet.

3.2.1.2 Regionales MONS

Die im vorangegangenen Abschnitt beschriebene Architektur liefert eine Lösung, die es einer beliebigen Institution technisch ermöglicht, eine Kopie des ONS-Root-Namensservers zu erhalten, was die Verfügbarkeit des ONS erhöht und was potenziell (aus globaler Perspektive) zu einem unstrukturierten Patchwork aus Bereichen mit höchst unterschiedlicher ONS-Root-Redundanz führen kann.

Abbildung 12: Regionales MONS

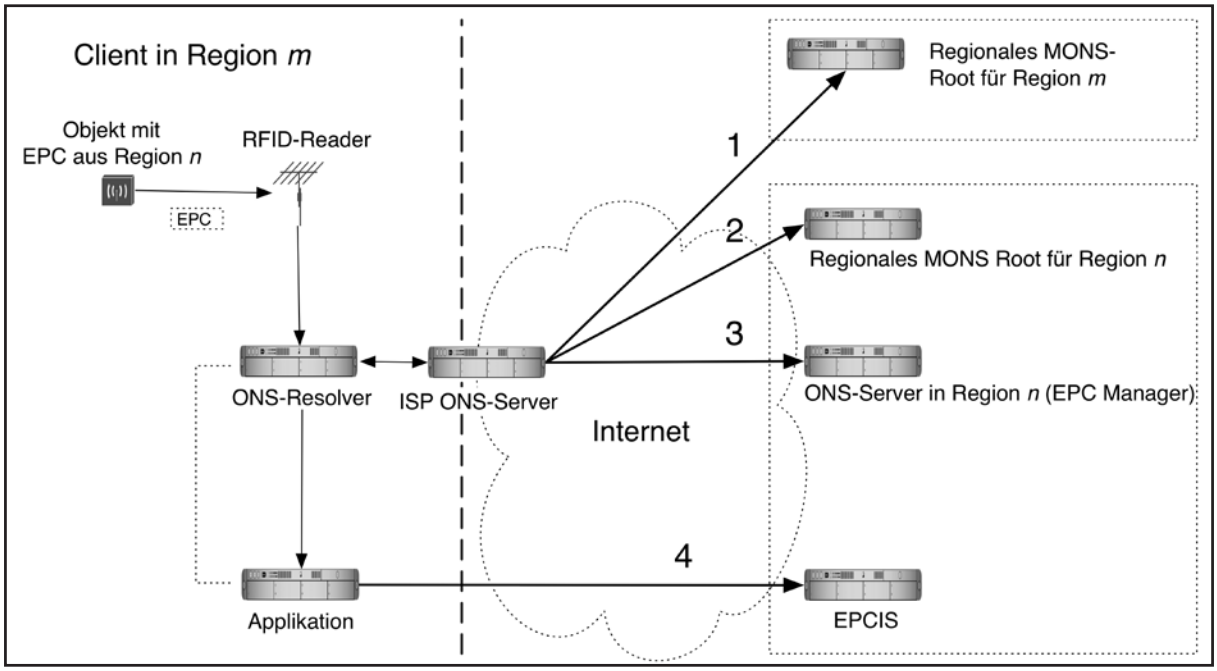


Aufgrund ihrer hohen Belastung könnten eventuell einige ONS-Roots nicht global zugänglich gemacht werden. Die Belastung eines Root-Namensservers ergibt sich einerseits aus der Frequenz der an ihn gerichteten Anfragen, andererseits aus Größe und Frequenz der Updates der Root Zone Files. Im Vergleich zur Zonendatei des DNS-Root, welches RRs über 1500 TLD-Namensserver enthält und gegenwärtig etwa 70 Kilobyte groß ist, wird die Datei für das ONS-Root RRs für alle ONS-Nameserver der EPC Manager, die bei EPCglobal registriert sind, enthalten. Da die Nutzung von RFID und EPC voraussichtlich stark zunehmen wird, ist zu erwarten, dass die Anzahl der EPC Manager schnell wachsen und in Millionen von RRs resultieren wird. Ferner könnte aufgrund von hoher Volatilität den RRs niedrigere Werte für ihre Gültigkeitsdauer (TTL-Parameter) zugewiesen werden als bei vergleichbaren RRs des DNS-Root. Als Ergebnis würden die ONS-RRs für kürzere Zeit zwischengespeichert, und eine größere Anzahl von Anfragen würde die ONS-Root Namensserver erreichen.

In diesem Abschnitt stellen wir eine weitere, stärkere Modifizierung der existierenden ONS-Architektur vor, die es erlauben wird, die Größe der Root-Zonendatei und die Häufigkeit ihrer Updates durch ihre Aufteilung zwischen mehreren *regionalen Root-Servern* zu reduzieren. Die Zonendatei eines jeden regionalen Root-Namenservers enthält RRs entsprechend den EPC-Managern, die zu der Region gehören, für die der Namensserver zuständig ist. Die Zugehörigkeit zu einer Region kann mittels der Adresse, unter der die Firma registriert ist, der regionalen GS1-Organisation, die das Company Prefix ausgestellt hat, oder anhand anderer Merkmale ermittelt werden.

Diese Architektur ist in Abbildung 12 abgebildet. Der zugehörige Prozess der EPC-Auflösung ist in der Abbildung 13 zu sehen. Falls der auflösende Namensserver und der EPC Manager (welcher dem EPC, der aufgelöst wird, entspricht) zu derselben Region gehören (n=m), dann wird der zweite Schritt übersprungen und der Auflösungsprozess ist fast identisch mit dem beim normalen ONS aus der Abbildung 2. Der regionale Root-Namensserver leitet die Anfrage an den Namensserver des EPC Manager weiter, welcher die Adressen der EPCIS zurückgibt. Anderenfalls, wenn n≠m, so wird die Anfrage an denjenigen regionalen Root-Namensserver umgeleitet, der für die Region n (Schritt 2) zuständig ist, der seinerseits die Anfrage an den Namensserver des EPC Manager weitergibt. Wir bezeichnen diese Architektur als *Regionales MONS*.

Abbildung 13: Abfrageprozess beim Regionalen MONS



Im Vergleich zum Auflösungsprozess des ONS stellt der Fall der Delegation der Anfrage von einem regionalen ONS Namensserver zum anderen (Schritt 2) einen zusätzlichen Auflösungsschritt dar. Daher erfordert dies eine Erweiterung des EPC-Schemas und die Einführung eines neuen Präfixes, das in diesem Schritt aufgelöst wird. Entsprechend den Standards zum Aufbau eines EPC wäre ein regionales Präfix, das auf das Land oder die Region der Herkunft des Produkts hinweist, eine nahe liegende Möglichkeit. Die Einführung eines solchen regionalen Präfixes erfordert eine Änderung der EPC-Kodierungsstandards, was zu einem kostenintensiven und langwierigen Prozess führen könnte.

Die bereits vorhandenen Konventionen enthalten allerdings bereits genug Informationen, um einen EPC eindeutig einer Region zuordnen zu können. Die ersten drei Stellen des EAN.UCC Firmenpräfixes identifizieren das Land der Mitgliedschaft des Unternehmens, z. B. sind die Codes 400-440 für Deutschland reserviert. Daher gibt es die Möglichkeit, diese Nummern ohne die Einführung neuer regionaler Präfixes zu nutzen, um die EPCs den zugehörigen Regionen zuzuordnen.

Der Resolver sieht das Regionale MONS immer noch als Hierarchie: Der MONS-Root seiner Region wird als eine Wurzel der gesamten Hierarchie aufgefasst. Wir bezeichnen eine solche Struktur als die relative Hierarchie. Ein regionaler Namensserver, der für die Region zuständig ist, in der die Auflösung passiert, wird ein relativer Root genannt. Das ermöglicht eine Implementierung des regionalen MONS innerhalb des DNS-Frameworks, was der Herangehensweise, die in der Spezifikation des ONS beschrieben wurde, entspricht.

Im Folgenden gehen wir davon aus, dass das regionale Präfix durch die ersten drei Ziffern des Firmenpräfixes definiert ist. Um auf den EPCIS, der die Daten über einen bestimmten EPC liefern könnte, zuzugreifen, wird dieser wie bei ONS in einen DNS-kompatiblen Namen übersetzt, allerdings müssen jetzt die ersten drei Ziffern des EPC Managers explizit durch Punkte abgetrennt und rechts von dem Rest des invertierten EPC-Namens platziert werden (z. B. 1734.453.400.sgtin.id.onsepc.com).

Angenommen, der DNS-Name des regionalen Namensservers, der für die Zone 400.sgtin.id.onsepc.com zuständig ist, sei ns1.mons.eu. Ein ONS-Client, der sich physisch in derselben Region befindet, wird so konfiguriert, dass er alle ONS-Anfragen an ns1.mons.eu (Schritt 1 in Abbildung 13), den er als relativen Root des regionalen MONS ansieht, weiterleitet. Dementsprechend würde ein Resolver, der zu einer anderen Region gehört, mit der Adresse eines anderen regionalen Roots konfiguriert werden, also diesen als ein relatives Root ansehen.

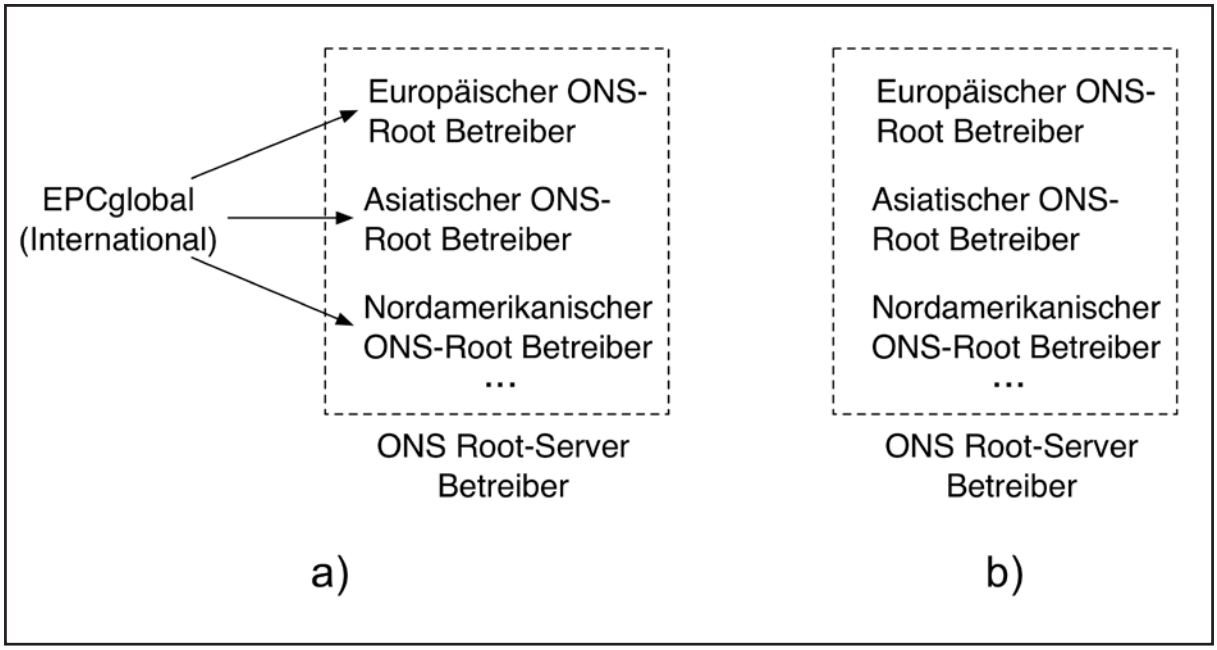
In diesem Beispiel wählten wir bewusst den Domainnamen des regionalen Root als Teil einer TLD (.eu) entsprechend der Region seiner Zuständigkeit. Diese Konvention vermeidet die Abhängigkeit von denjenigen Institutionen, die die regionale Domain des Namensservers administrieren, und schließt die Möglichkeit einer indirekten Root-Blockade über die Kontrolle von DNS-Namen von deren Seite aus.

Indem bestimmte Namensserver eindeutig Regionen zugewiesen werden, verlagert das regionale MONS natürlicherweise die stärkste Belastung auf diejenigen Namensserver, die für ökonomisch entwickelte oder industrielle Länder zuständig sind, da die regionalen Präfixe solcher Regionen in den meisten EPCs vorkommen werden und von dort ebenfalls die meisten Anfragen kommen werden. Ferner können Regionen, deren Exportwerte zu niedrig sind, oder die nicht daran interessiert sind, ihre eigenen regionalen MONS-Roots zu pflegen, diese Verantwortung an Dritte delegieren, ähnlich wie es manchmal mit den TLDs im DNS gehandhabt wird. Sobald sich ihre Situation ändert, können diese Länder ihren reservierten Teil des Systems durch geringfügige Änderungen in der Tabelle der regionalen MONS-Roots (MONS-Root-Zonendatei) zurückerhalten.

3.2.1.3 Machtstruktur

Abbildung 14 illustriert mögliche Machtstrukturen für die in diesem Abschnitt beschriebenen MONS-Architekturen. Jeder replizierte oder regionale ONS-Root-Server wird von einer korrespondierenden, regionalen Firma unterhalten. Im Falle des Replizierten MONS besteht immer noch die Notwendigkeit einer zentralen Instanz (z. B. durch EPCglobal in diesem Beispiel). Beim Regionalen MONS wird keine zentrale Instanz zur Koordinierung benötigt, da jedes Regionale Root unabhängig von den anderen betrieben wird und die Rolle von EPCglobal auf einfache Verwaltungsaufgaben beschränkt wäre.

Abbildung 14: Beispiel einer möglichen Machtstruktur, a) Repliziertes MONS b) Regionales MONS



3.2.1.4 Ökonomische Aspekte

Das in Abschnitt 3.1.1.3 erwähnte Anreizproblem bleibt relevant für die hier erwähnte MONS-Architektur. Die Dezentralisierung von MONS könnte jedoch zu einem flexibleren Gebührensystem führen, da die meisten Kosten, die durch die Wartung von ONS-Root-Servern entstehen, von den entsprechenden regionalen Organisationen (z. B. regionale GS1-Abteilungen) getragen werden. Momentan werden die Gebühren für Unternehmen mit einem Umsatz von bis zu 250 Millionen USD von den lokalen GS1-Abteilungen festgelegt, während die Gebühren für Unternehmen mit einem Umsatz von mehr als 250 Millionen USD durch die EPCglobal-Preisliste festgelegt werden.

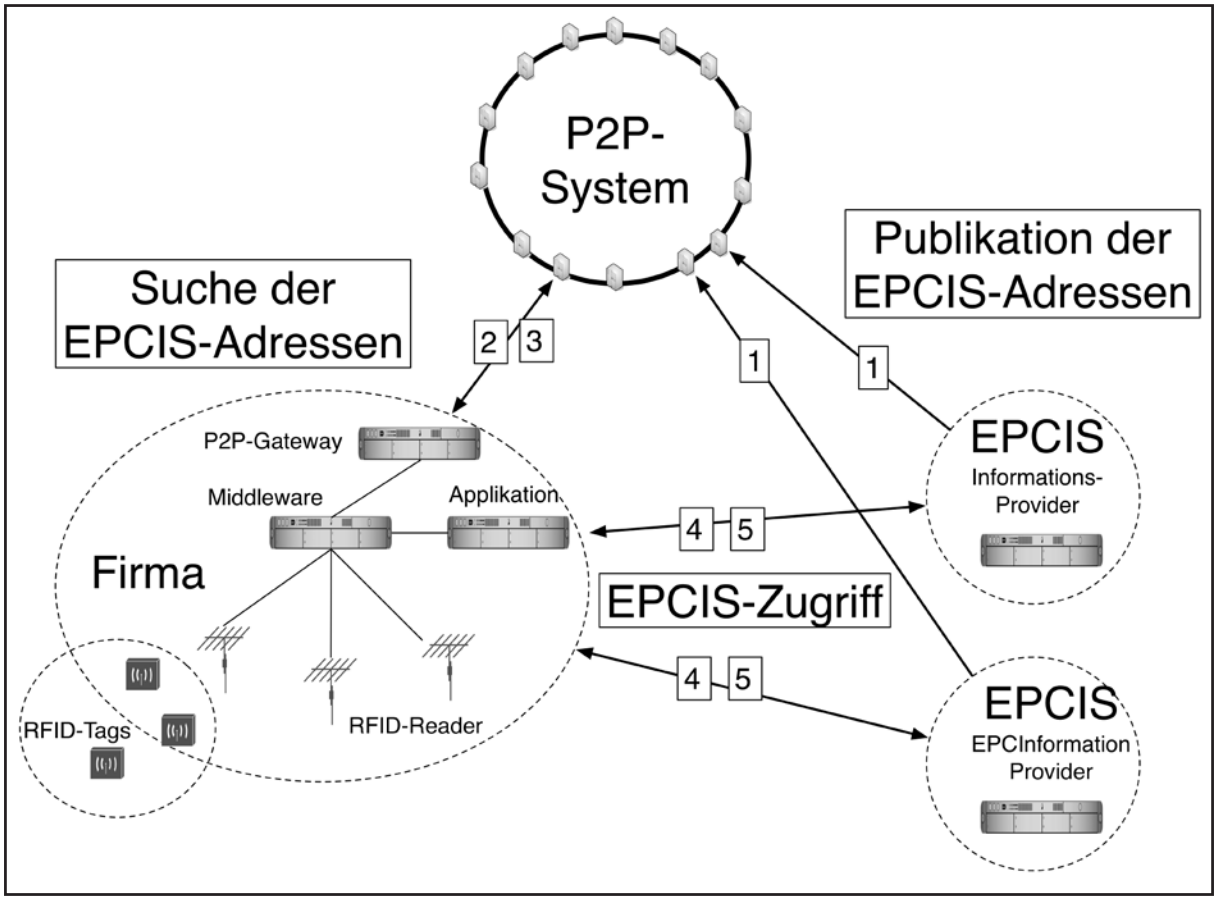
3.2.2 Sicherheit

MONS ist nicht dafür entworfen worden, eine Lösung für die generellen Probleme von Integrität, Verfügbarkeit und Vertraulichkeit im ONS zu liefern. Es ist eine DNS-basierte Architektur, deren Hauptziel es ist, das Unipolaritätsproblem zu lösen. Die Integritätsprobleme können allerdings mit dem zusätzlichen Einsatz von DNSSEC (siehe Abschnitt 3.4) gelöst werden.

3.3 Peer-to-Peer ONS

Alternative Architekturen zum ONS können auf Peer-to-Peer-Architekturen (P2P) basieren, die eine wesentlich flexiblere Handhabung der Rollen Client und Server ermöglichen, als es in klassischen verteilten Systemen möglich ist. Beide Rollen können jeweils gleichzeitig von allen beteiligten Knoten in einem Netzwerk ausgeübt werden. Peer-to-Peer-Netzwerke sind also wesentlich weniger zentral und bestehen üblicherweise aus gleichberechtigten Partnern, die auch Knoten (Nodes) genannt werden. Die EPCIS-Adressen würden als Dokumente in diesen P2P-Systemen gespeichert und wieder abgerufen werden können (siehe Abbildung 15).

Abbildung 15: Beispiel einer P2P-ONS Architektur



3.3.1 Technik und Organisation

Man unterscheidet oft zwischen strukturierten und unstrukturierten P2P-Systemen. Im unstrukturierten Fall wächst das P2P-System im Wesentlichen ungesteuert, und die Zuordnung von Daten zu Knoten ist nicht festgelegt. Vorteil dieser Systeme ist die Möglichkeit, mit einer hohen Fluktuation der teilnehmenden Knoten umgehen zu können, Nachteil, dass Suchanfragen bei hoher Teilnehmerzahl sehr ineffektiv werden, da sie im Wesentlichen ungerichtet durch das gesamte Netz propagiert werden müssen. Abhilfe schaffen sogenannte hybride P2P-Systeme, wo zentrale Indexserver die Suche erleichtern, aber zugleich leichte Ziele für Angriffe auf das System darstellen.

3.3.1.1 Vorteile und Herausforderungen von Peer-to-Peer Systemen

Eine sehr vielversprechende Forschungsrichtung, besonders auch für Infrastrukturnetzwerke, bilden strukturierte P2P-Systeme auf Basis verteilter Hashtabellen (Distributed Hash Table, DHT).[19] DHT-Systeme sind im Allgemeinen auch bei großer Teilnehmerschaft sehr gut skalierbar, robust gegenüber Ausfällen und gezielten Angriffen, vermeiden ausgezeichnete Knoten (etwa Wurzeln einer Hierarchie, wie das ONS-Root) und somit einen „single point of failure", und verteilen systematisch die Speicherbelastung und Verantwortlichkeit zwischen den Teilnehmern. Ermöglicht wird dies durch die Bildung einer topologischen „Overlay"-Struktur, in die sich Knoten und Datenadressen systematisch einfügen und wieder austragen lassen, ohne dass eine zentrale Instanz dazu notwendig wäre oder das Netzwerk global geändert werden müsste. Eine DHT bietet einfache Speicher- und Suchfunktionalität auf Basis einer Korrespondenz zwischen Suchschlüsseln, Daten und den Computern selbst, die das Netzwerk bilden.

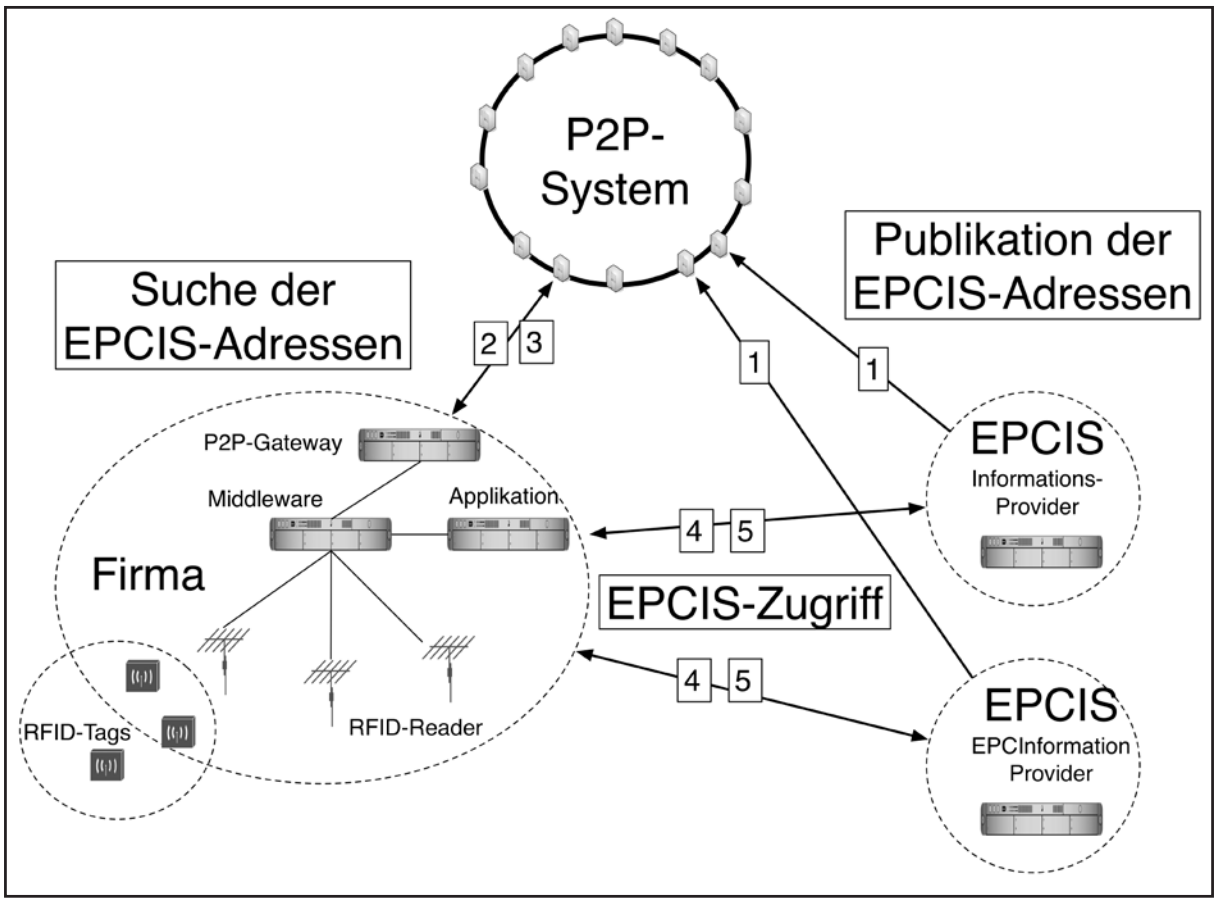
Bei der Nutzung von P2P-Systemen gibt es allerdings auch neue Herausforderungen. Einfach auf eine P2P-Architektur für ONS umzustellen, selbst wenn die beteiligten Knoten Infrastrukturrechner von Firmen und keine einfachen Desktop-PCs sind, würde die Integrität der gespeicherten Dokumente nicht garantieren, könnte allerdings die Vertraulichkeit und Anonymität der Anfragen unter Umständen erhöhen, da auf eine zentrale erste Anfrage-Instanz wie den ONS-Root oder mehrere Regionale MONS-Roots verzichtet würde. Andere Angriffsvektoren auf die Vertraulichkeit der Anfragen, wie etwa das Mitlesen von IP-Paketen, wären immer noch relativ leicht durchführbar. Es bedarf also im Allgemeinen weiterer Schutzmechanismen, um neben erhöhter Robustheit und hervorragender Skalierbarkeit weitere Vorteile gegenüber dem klassischen ONS in P2P-Architekturen umzusetzen. Exemplarisch sei im Folgenden ein Beispiel für P2P-ONS vorgestellt, das zusätzliche Sicherheitsfunktionalität bereitstellt.

3.3.1.2 Object-Information Distribution Architecture (OIDA)

In diesem Abschnitt wird ein DHT-basiertes P2P-ONS namens Object-Information Distribution Architecture (OIDA) vorgestellt.[20] OIDA soll als weltweites Infrastruktur-Netzwerk für ONS fungieren und beinhaltet die folgenden wichtigen Ideen: Jede an der Teilnahme interessierte Firma stellt dedizierte OIDA-Knoten bereit, d. h. Computer, die wie bei DNS- oder ONS-Servern aus Performanz- und Sicherheitsgründen nur eine Aufgabe zu erfüllen haben. Diese Knoten bilden ein Overlay-Netzwerk auf Basis einer fest gewählten verteilten Hashtabelle (DHT), wobei eine kryptografische Hashfunktion EPCs und physische Knoten in einer Topologie von Overlay-Identifikatoren abbildet, deren spezifische Eigenschaften von der spezifisch gewählten DHT abhängen. Diese pseudozufällige Zuordnung von Daten und Speicherknoten bewirkt eine gleichmäßigere Lastverteilung als beim ONS, wo z. B. das ONS-Root voraussichtlich besonders stark belastet wird. Ebenso wird die Möglichkeit reduziert, gezielte Angriffe gegen die ONS-Daten spezifischer Firmen durchzuführen.

[19] Siehe [BKK03]
[20] Siehe [FG07]

Abbildung 16: Abfrageprozess bei OIDA

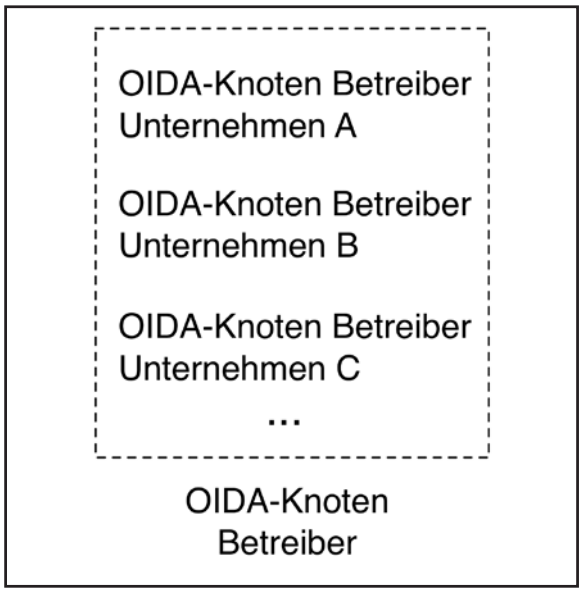


Die DHT übernimmt das Routing von Anfragen zu demjenigen Knoten, auf dem die gewünschte Information gespeichert ist (Abbildung 16). Zusätzlich ist die DHT-Software für das dezentrale Management von Protokollen zuständig, die das Hinzufügen und Entfernen von Knoten, sowie die Reparatur der DHT bei spontanen Knotenausfällen regeln.

3.3.1.3 Machtstruktur

Abbildung 17 zeigt mögliche Machtstrukturen bei der OIDA-Architektur. Jeder OIDA-Knoten wird von einem Unternehmen betrieben, das ein Interesse daran hat, seine Produktinformationen global adressierbar zu machen. Es gibt hier keine speziellen Vermittler (wie z. B. ONS-Root-Betreiber) in der Architektur, da OIDA-Knoten untereinander die Anfragen nach Adressen geeigneter EPCIS direkt und korrekt zustellen.

Abbildung 17: Machtstruktur bei OIDA



3.3.1.4 Ökonomische Aspekte

Das Kostenverteilungsproblem aus Abschnitt 3.1.1.3 bleibt auch bei der OIDA-Architektur relevant. Da aber diese Architektur keine Infrastruktur voraussetzt, die von Dritten betrieben wird wie etwa die Root-Server beim ONS, könnten die Beitragskosten signifikant gesenkt werden oder gar vollkommen entfallen.

Andererseits führt eine solche verteilte Architektur zu neuartigen Anreizproblemen. Da ein OIDA-Knoten mit hoher Wahrscheinlichkeit gar keine eigenen Adressdaten speichert, sondern die anderer Firmen, gibt es keine unmittelbaren, direkten Anreize, adäquat an OIDA zu partizipieren, d. h. die Knoten adäquat und korrekt zu betreiben, ihre Verfügbarkeit zu garantieren, für Updates, Hardwareupgrades und ausreichende Konnektivität zu sorgen, um die Anwortzeiten gering zu halten.

Dies betrifft sowohl OIDA als auch andere ähnliche P2P-Architekturen, in denen die Daten vom Informationsprovider getrennt gespeichert werden. Die meisten P2P-Netze, die in der Praxis existieren, werden nicht als Teil einer kritischen Infrastruktur aufgefasst, sondern werden von Freiwilligen betrieben, und ihre Anwendungsgebiete erfordern keine besonderen Ausgaben und Wartungskosten.

Im Falle eines P2P-basierten Namensdienstes könnten zusätzliche Maßnahmen notwendig werden, um das korrekte Funktionieren der Hardware und des Overlay-Netzes zu überprüfen und zu garantieren, dass ein solches System den Namensdienst für tausende von Firmen übernehmen kann. Geeignete Verträge und ein Monitoring-Verfahren für die Verfügbarkeit wären entsprechende Optionen. Auch bei P2P-ONS kann somit eine zentrale Instanz notwendig sein, die ein adäquates Partizipieren der Teilnehmer sicherstellt.

3.3.2 Sicherheit

Auf den OIDA-Knoten werden die Dokumente mit den EPCIS-Adressen in verschlüsselter Form und in Verbindung mit einer digitalen Signatur des Informationsproviders abgespeichert, was eine Überprüfung ihrer Integrität und Authentizität durch den Endanwender ermöglicht. Die Dokumente sollten die IP-Adressen der EPCIS und nicht ihre DNS-Namen erhalten, um von der Authentizität des globalen DNS unabhängig zu sein.

Um die Signaturen für die Daten skalierbar umzusetzen, könnten eine zentrale Zertifizierungsstelle etwa bei EPCglobal, eine hierarchische Vertrauensinfrastruktur wie zum Beispiel DNSSEC, oder ein dezentrales „Web of Trust“ wie bei PGP, das z. B. für Email benutzt wird, zum Einsatz kommen. Diese Infrastruktur muss ihrerseits auf ihre Sicherheit und ökonomisch-politischen Implikationen untersucht und ggf. entsprechend weiterentwickelt werden (siehe auch Abschnitt 3.4 zu DNSSEC).

In der folgenden Tabelle sind die wesentlichen Sicherheitsmerkmale von OIDA und ihre Auswirkungen dargestellt.

Tabelle 6: Sicherheitsmerkmale von OIDA

Merkmal	Auswirkung	Positiver Effekt auf:
DHT-Architektur (Peer-to-Peer)	Kein „Root“, keine ausgezeichneten Knoten. Kein „single point of failure/control/attack“	Verfügbarkeit, Multipolarität
	Entkoppelung von Informationsprovider und Speicherort der Information. „Zufällige“ Auswahl von Dokumenten auf jedem OIDA-Knoten ► Geringere Motivation zur systematischen Logfileanalyse durch OIDA-Knoten	Vertraulichkeit der Clientanfrage (gegen Betreiber und ISP des OIDA-Knotens)
Konvention zur Replikation	Nahezu beliebige Anzahl von Kopien der Adressdokumente	Verfügbarkeit, Multipolarität
Digitale Signaturen auf den Dokumenten	Authentizität der Dokumente vom Client überprüfbar, auch wenn aus unsicherer Quelle bezogen	Integrität der Dokumente (gegen Modifikation durch Dritte)
Optional: PKI zur Absicherung der OIDA-Knoten (Node PKI)	Erhöhung Integrität gegen externe Angreifer, die die DHT manipulieren wollen (Publikationsphase, Routing, Nachrichten über Nicht-Existenz von Dokumenten)	Integrität der DHT, Verfügbarkeit der Dokumente
Kryptografische Hashfunktion der DHT	EPC wird nicht im Klartext übertragen	Vertraulichkeit der Clientanfrage (gegen alle ISP, Internet Backbone, OIDA-Knoten)
Verschlüsselung der Dokumente	Die Antwort wird nicht im Klartext übertragen. ► Kein indirekter Rückschluss auf die Anfrage möglich	Vertraulichkeit des Dokuments (gegen Dritte) Vertraulichkeit der Anfrage (gegen Dritte und Informationsprovider)
Rekursives Routing in der DHT	Bei der Kommunikation innerhalb der DHT bis zum zuständigen OIDA-Knoten bleibt die Identität des Clients verschleiert	Anonymität des Clients (gegenüber Provider, OIDA-Knoten und vielen Dritten – aber nicht gegen ISP des Clients oder sein benutztes OIDA-Gateway)
SSL/TLS zwischen Client (OIDA-Proxy) und OIDA-Gateway	Verschlüsselung und Authentifizierung der Verbindung zu den OIDA-Gateways	Vertraulichkeit und Integrität (gegen ISP des Clients, Internet Backbone, aber nicht gegen OIDA-Gateway)

Zusammenfassend sei festgehalten, dass OIDA die Auflösung von EPCs zu EPCIS-Adressen vollständig von der klassischen DNS-Infrastruktur und ihren Protokollen entkoppeln könnte, was auch deren Überlastung durch neue Anwendungen auf Basis des Internets der Dinge vermeiden würde. Dabei bietet OIDA erhöhte Vertraulichkeit und Anonymität sowie einfache Replikationsmechanismen zur Erhöhung der Datenverfügbarkeit, und vermeidet unter der Annahme einer globalen Teilnehmerschaft unipolare Machtstrukturen. Auch in P2P-Infrastrukturnetzen wie OIDA kann eine zentrale Instanz, etwa ein unabhängiges internationales Gremium oder Konsortium, für organisatorische Aufgaben, Sicherheitsinfrastrukturen, Verfügbarkeits-Monitoring und Softwareupdates wichtig sein.

Für alle Namensdienstarchitekturen (z. B. ONS, MONS, OIDA) muss die Frage nach der Sicherheit und Multipolarität der flankierenden technischen Sicherheitsinfrastrukturen berücksichtigt werden. Ein wichtiges Beispiel einer solchen Infrastruktur ist DNSSEC, das im nächsten Abschnitt vorgestellt wird.

3.4 DNSSEC – Schutzfunktion und neue Herausforderung

Eine wichtige Technik, Authentizität und Integrität beim DNS abzusichern, ist unter dem Namen DNSSEC (DNS Security Extensions) bekannt.[21] Auch für die Gewährleistung von Integrität und Authentizität von ONS und DNS-basierten Varianten wie MONS kann DNSSEC eine wichtige Rolle spielen, ist aber ebenfalls mit neuen Herausforderungen verbunden.

Zunächst bietet DNSSEC die Möglichkeit gegenseitiger Authentifizierung von DNS-Servern auf Basis geteilter Geheimnisse. Dieses Verfahren ist jedoch nur bedingt skalierbar. Eine wichtigere in DNSSEC integrierte Technik stellt Authentizität und Integrität der eigentlichen DNS-Daten sicher. Dabei werden öffentliche Schlüssel (Public-key Kryptografie) und Signaturen verwendet, die über Ketten vertrauenswürdiger Instanzen verifiziert werden.

Gegenwärtig wird DNSSEC jedoch noch relativ selten in der Praxis eingesetzt. Gründe dafür können in der Schwierigkeit liegen, Vertrauensbeziehungen außerhalb kleiner Vertrauensinseln („Islands of Trust“) aufzubauen. Zur Gewährleistung von Datenintegrität im ONS durch DNSSEC wäre jedoch ein flächendeckender Einsatz notwendig. Um diese Herausforderung skalierbar zu bewältigen, könnte man parallel zur DNS-Namenshierarchie einen Baum von Vertrauensbeziehungen schaffen, sodass man in der Theorie nur wenige öffentliche Schlüssel (z. B. des DNS-Roots) kennen muss, um eine Verifizierung der DNS-Daten durchzuführen, indem man dem Delegationspfad folgt und die Vertrauenskette auf Lückenlosigkeit überprüft.

Selbst wenn DNSSEC eine Verschlüsselung von DNS-Informationen ermöglichen könnte, was bisher bei der Verwendung in den entsprechenden Standards explizit ausgeschlossen wird, ließe sich dennoch zumindest der Company Identifier (EPC Manager) eines angefragten EPC durch Analyse des Netzwerkverkehrs bestimmen. Dies wäre durch eine einfache Beobachtung der IP-Adressen möglich, an die ONS-Anfragen und nachfolgende EPCIS-Kommunikation gesendet werden. DNSSEC bietet ebenso keinerlei Schutz für die Verfügbarkeit des Dienstes.

[21] Siehe [RFC4003]

Ein in jüngerer Zeit diskutiertes politisches Thema ist die Frage, welche Institution die Kontrolle über die Schlüssel der DNS-Rootzone innehaben sollte, die zurzeit US-amerikanischer Aufsicht unterliegt.[22] Wenn ONS multipolar umgestaltet wird, sollte dies parallel zu der zugehörigen Vertrauensinfrastruktur DNSSEC geschehen, wenn sie bei ONS Verwendung finden soll. Dabei muss beachtet werden, dass sämtliche DNS-Namen, die in den URL-Einträgen der ONS-RR vorkommen können (welche im Prinzip beliebig sind), durch DNSSEC authentisch mit ihren IP-Adressen verbunden werden müssen. DNSSEC für ONS darf sich also nicht nur auf die Absicherung des ONS-Teilbaums des DNS beschränken (onsepc.com samt Unterdomänen), da sonst Lücken in der Integritätssicherung bestünden.

3.5 Die Bedeutung von IPv6

Das zurzeit etablierte Internetprotokoll IPv4 dient dem korrekten Adressieren und der Wegeleitung (Routing) von Datenpaketen im Internet. Um am Internet teilzunehmen, sind IP-Adressen für die beteiligten Kommunikationspartner notwendig. Diese IP-Adressen werden für IPv4 in den nächsten Jahren knapp.

Bereits im Jahr 1995 hat die Internet Engineering Task Force (IETF) einen Nachfolger für das Internetprotokoll IP bestimmt: IPv6.[23] Bisher ist die ältere Version IPv4 dominant geblieben, wobei allerdings vor allem in asiatischen Ländern mit knappem IPv4-Adressraum und bei mobilen Geräten bald ein großflächiger Einsatz von IPv6 notwendig werden könnte.

IPv6 bietet viele Vorteile gegenüber der älteren Version. Da die Adressen bei IPv6 128 Bit lang sind, erhält man einen wesentlich umfangreicheren Adressvorrat als bei IPv4 mit seinen 32-Bit Adressen. Die dadurch mögliche großzügige Zuteilung von Subnetzen führt u. a. auch zu einer Vereinfachung der internetweiten Routingtabellen. Ein vereinfachter IP-Header und die Auslagerung von Optionen in sogenannte „Extension Headers“ und eine Vermeidung von Fragmentierung entlasten die Router zusätzlich. In der Form von IPSEC (IP Security) ist ein Teil der Sicherheitsprotokolle von IPv6 für IPv4 rückportiert worden, allerdings ist ihre Implementierung bei IPv6 verbindlich.

Von Beginn an war die Mobilität von IP-vernetzten Geräten eine wichtige Entwurfskomponente bei IPv6, man erwartete schon damals ihren großen Anteil am Internet. Neben der Autokonfiguration, der automatischen Generierung einer IP-Adresse aus einem von Routern bekanntgegebenem „Präfix“, spielt dabei vor allem das Protokoll Mobile IPv6 eine große Rolle, das besonders mobile Geräte mit häufig wechselnden Aufenthaltsorten und Netzanbindungen unterstützt.[24]

22 Siehe z. B. die gesammelten Quellen bei heise.de:
http://www.heise.de/security/VeriSign-will-DNSSEC-Schluessel-ein-bisschen-teilen--/news/meldung/116903 sowie
http://www.heise.de/newsticker/IGF-Schlagabtausch-zum-Einfluss-der-Regierungen-im-DNS--/meldung/120035.

23 Siehe [RFC2460], [Los04].

24 Siehe [Sol04].

Für ein zukünftiges, echtes Internet der Dinge jenseits von RFID, d. h. mit vollständiger IP-Implementierung auf den Chips, die zu den Objekten gehören, könnte eine Konvergenz auf dem Network Layer zu IPv6 stattfinden – unabhängig von dem jeweils benutzten physischen Kommunikationsmedium (z. B. RFID, WLAN, Bluetooth, WiMax oder UMTS). Geplante Migrationsprozesse und sogenannte Tunnelverfahren, bei denen z. B. IPv6-Pakete in IPv4-Pakete transportiert werden, können die Verbindung zur etablierten IPv4-Infrastruktur ermöglichen und die Integration der Smart Objects in bestehende Netze erleichtern.

Ein Namensdienst wie ONS würde in einem solchen Szenario nicht nur der Suche nach EPCIS dienen, sondern auch dazu, die IP-Adressen der Objekte selbst mithilfe ihres ONS-Namens zu finden, um sie aus der Ferne des Internets direkt kontaktieren zu können. In einem solchen Szenario aus Milliarden IPv6-vernetzter Objekte könnten noch größere Herausforderungen an die Namensdienst-Infrastrukur bezüglich Skalierbarkeit und Abfragenlast entstehen, als beim Einsatz von ONS nur für RFID-Tags oder den Anforderungen an DNS im heutigen Internet.

4. Ergebnisse der Interviews

Im Rahmen dieser Studien wurden Gespräche mit Experten aus Wirtschaft und Wissenschaft geführt, in denen ihre Einschätzung der gegenwärtigen ONS-Diskussion eingeholt werden sollte. Folgende Unternehmen stellten sich freundlicherweise für Interviews bereit: CBR (Modetextilien), Deutsche Post World Net (Logistik), Gerry Weber (Modetextilien), IBM Deutschland (Informationstechnik und Systemintegration), Kaufhof (Handel), Lufthansa Technik Logistik (Luftfahrt, Logistik), METRO Group Information Technology (IT-Dienstleistung für den Handel), Psipenta (Software und Systemintegration), Robert Bosch (Medizintechnik), Seeburger (Software und Systemintegration), und Volkswagen (Automobil). Ferner wurden Gespräche mit den Verbänden AIM-D (Identifikationssysteme) und VDMA (Maschinenbau) sowie mit dem Bremer Institut für Produktion und Logistik an der Universität Bremen (BIBA) geführt.

ONS war vielen kontaktierten Unternehmen unbekannt, oder sie waren zumindest nicht hinreichend mit dem Thema vertraut. Ein großer deutscher Automobilhersteller und ein großer Telekommunikationsprovider teilte auf Nachfrage mit, dass man zum Thema keine öffentliche Stellungnahme abgeben will. Diverse Mittelständler waren zwar prinzipiell für ein Interview offen, waren über die Materie aber nicht im Detail informiert. Insbesondere die Anwender unter den Interviewpartnern sind damit insofern eine Positivauswahl, als sie in der Regel schon RFID-Projekte durchgeführt haben und durchgehend über tiefere Kenntnisse der RFID-Technik sowie der gegenwärtigen Diskussion um ONS verfügen.

Der überwiegende Teil der Gesprächspartner hat um eine vertrauliche Behandlung seiner konkreten Einschätzungen gebeten, sodass im Folgenden generell die Aussagen nicht einzelnen Interviewpartnern zugeordnet werden.

Der vorab übermittelte Problemaufriss (siehe Kapitel 2) wurde von den Interviewpartnern als verständlich und in der Fokussierung auf die fünf Problemdimensionen (Unipolarität, ONS-interne Machtstrukturen, Integrität, Verfügbarkeit, Vertraulichkeit und Anonymität) überwiegend als umfassend und zielführend bewertet. Ein Gesprächspartner wies jedoch darauf hin, dass das EPCglobal Network und der ONS nicht mit dem Internet der Dinge gleichgesetzt werden können. Das EPCglobal Network und der ONS seien lediglich eine erste Ausprägung einer Infrastruktur für das Internet of Things. In fast allen Interviews wurde ergänzend auch die gegenwärtige Relevanz des ONS thematisiert.

Allgemeine Relevanz des ONS

Übereinstimmend schätzen die Anwender unter den Interviewpartnern die *gegenwärtige* Relevanz des ONS für ihr Unternehmen bzw. ihre Branche als eher gering ein. Zur Begründung wird auf noch nicht gegebene breite Ausrüstung von Konsumprodukten mit RFID-Tags, auf die teilweise schon bestehende Integration von RFID in bestehende EDI-Systeme und auf den Wettbewerb von RFID mit alternativen Identifikationssystemen hingewiesen. Die Einschätzung, ob und wann ONS bzw. das EPCGlobal-Netzwerk für die Anwender ein strategisch relevantes Thema wird, ist uneinheitlich. Die Aussagen reichen von der Nichtabsehbarkeit eines Mehrwerts durch ONS bis zur Einschätzung, dass mit ONS bzw. dem EPCGlobal-Netzwerk und seinen Diensten veraltete EDI-Systeme abgelöst werden könnten.

Die Technikanbieter unter den Lösungspartnern beziehen sich bei der Einschätzung der Relevanz des ONS bzw. des EPCglobal-Netzwerks durchweg auf das Urteil ihrer Kunden, eigene strategische Interessen wurden nicht thematisiert.

Unipolarität und Machtstrukturen

Sofern das technische Ausfallrisiko eines zentralen ONS-Dienstes überhaupt von den Interviewpartnern thematisiert wird, wird es als gering und beherrschbar eingeschätzt. Das politische Risiko wird sehr unterschiedlich gesehen. Ein Teil der Anwender sieht den ONS-Dienst für die Nutzung von RFID bzw. EPCglobal in der eigenen Branche als nicht relevant an, so dass überhaupt keine Gefahr im Betriebsmodell gesehen wird. Andere Interviewpartner verweisen auf die Gefahren eines privatwirtschaftlichen ONS-Betreibers unter einer nationalen Jurisdiktion, etwa willkürliche Leistungsbegrenzungen oder Systemabschaltungen. Als Negativbeispiele werden der DNS-

Dienst für das Internet und der Lokalisierungsdienst GPS genannt. Ein Gesprächspartner verweist auf etwaige Akzeptanzprobleme eines US-dominierten EPCglobal-Systems in Russland und im nahen Osten.

Andere Befragte sehen dagegen die Gefahr eines Missbrauchs des ONS-Dienstes durch einen US-basierten Betreiber als nicht existent an. Das wird insbesondere damit begründet, dass das EPCglobal Network lediglich eine Ergänzung etablierter und vertrauenswürdiger IT-Infrastrukturen für die Datenkommunikation zwischen Unternehmen sei. Die direkte Eins-zu-Eins-Kommunikation mit bekannten Partnern, in der der ONS-Dienst verzichtbar ist, werde auch in absehbarer Zukunft der Regelfall bleiben.

Mehrere Interviewpartner erachten es als kritisch, dass die Entwicklung von EPCglobal nicht durch eine neutrale Standardisierungsorganisation betrieben wird, sondern von einem Industriegremium mit Fokus auf Handel und Konsumgüterindustrie. Ebenso werden zum Teil die Gebühren für die Nutzung des EPCglobal-Netzwerks als Nutzungsbarriere, insbesondere für KMU, eingeschätzt.[25]

Integrität, Verfügbarkeit, Vertraulichkeit und Anonymität

Die meisten Befragten sehen für ihr Unternehmen bzw. ihre Branche ein differenziertes Berechtigungs- und Zugriffskonzept als wesentliche Voraussetzung für ein praxistaugliches EPCglobal-Netzwerk an. Die potenzielle Gefahr einer Profilbildung zu Produkten und Unternehmen wird mehrfach erwähnt. Prinzipielle technische Hürden für die Umsetzung einer entsprechenden Sicherheits-Infrastruktur werden in der Regel nicht gesehen. Mehrere Unternehmen verweisen jedoch auf die große Bedeutung allgemeiner Richtlinien für die Umsetzung und den Betrieb eines solchen Sicherheitssystems sowie auf deren Umsetzung: Jedes Unternehmen im Netzwerk muss den Sicherheitsmaßnahmen der anderen Partner vertrauen können. Ein Gesprächspartner verweist auf die gegenwärtig vom BSI erstellte *Technische Richtlinie für den sicheren RFID-Einsatz*. Die Sensibilisierung hinsichtlich des Schutzes von etwaigen personenbezogenen Daten ist hoch. Zwei Befragte geben sogar an, dass sie Anwendungen, in denen personenbezogene Daten anfallen, bewusst nicht verfolgen.

Die Detailfragen nach den technischen Kernelementen der IT-Sicherheit – Integrität, Verfügbarkeit, Vertraulichkeit und Anonymität – wurden von den Interviewpartnern nur teilweise thematisiert. Das dürfte insbesondere auf das noch frühe Stadium der Entwicklung des EPCglobal Network und des ONS-Dienstes zurückgehen sowie auf das Vertrauen, dass sich bekannte Lösungen für diese Fragestellungen aus anderen Anwendungskontexten prinzipiell übernehmen lassen.

[25] Vom BIBA wurde im Gespräch ein System zur Trennung von Produkt- und Informationskosten thematisiert [Uckel08]. Durch die Implementierung eines Billing-Systems (beispielsweise auf der Grundlage von Readern, die mit einer SIM-Karte ausgestattet sind, die Lese-Events protokollieren und kumuliert abrechnen) könne so eine „kontrollierte Transparenz“ geschaffen werden. Auf diese Weise wäre es möglich, bestimmte Informationen frei und kostenlos zugänglich zu halten, während andere Informationen kostenpflichtig und damit nicht mehr uneingeschränkt zugänglich sind. Entsprechend könnten Zugriffe auf bestimmte Nutzer beschränkt und andere (z. B. Wettbewerber) ausgeschlossen werden. Darüber hinaus würde mit der Trennung von Kosten auch die Qualität der Daten/Informationen indirekt gesichert, da für nutzlose Infos keine Zahlungsbereitschaft bestehe.

Für die meisten Interviewpartner ist die Integrität eine notwendige Eigenschaft für das EPCglobal-Netzwerk und dessen Dienste. Insbesondere müsse auch bei einer Verteilung des ONS-Diensts die Eineindeutigkeit bei der Zuordnung der EPC-Nummern zu den Objekten gewährleistet sein. Bei der Verfügbarkeit wurde auf den (bekannten) Betrieb gespiegelter ONS-Dienste verwiesen, mit denen ein single point of failure vermieden werde könne. Zur Bedeutung von Vertraulichkeit und Anonymität im EPCglobal Network gab es nur wenige Antworten, die dann diesen Aspekten überwiegend eine hohe Bedeutung zumessen.

Unterstützung durch die Öffentliche Hand

In der Mehrzahl sehen die Befragten keinen Bedarf an Unterstützung oder Regulierung des ONS-Dienstes oder des EPCglobal Networks durch die Öffentliche Hand. Die Unternehmen, die staatliche Aktivitäten wünschen, sind jedoch gerade die, die dem EPCglobal Network und ONS eine höhere Relevanz zusprechen. Als wünschenswerte öffentliche Aktivitäten werden von diesen Gesprächspartnern genannt: die Unterstützung von Alternativen zum ONS, beziehungsweise des Übergangs zu einem neutralen Betrieb des ONS und des zukünftigen Internet der Dinge sowie die Moderation eines ONS-Standardisierungsdialogs. Gleichzeitig sprechen sich aber auch diese Interviewpartner für eine Technikentwicklung durch die Wirtschaft aus, öffentliche FuE-Projekte werden als eher ungeeignet angesehen. Allerdings wurde die öffentliche Unterstützung von frühen prototypischen Lösungen (first user action) als geeignet erachtet.

Von einem Gesprächspartner wurde bemängelt, dass die gesellschaftspolitischen Anforderungen an eine Selbstregulierung von Netzwerkdiensten wie dem ONS zu vage fomuliert seien. Hier sei eine Konkretisierung wünschenswert, die die Politik im Gespräch mit Unternehmen und Standardisierungsgremien erarbeiten solle.

5. Handlungsempfehlungen

Befund

Die zukünftige Bedeutung der ONS-Thematik wird insbesondere von den Unternehmen, die sich schon intensiver mit dem Thema beschäftigt haben, deutlich gesehen. Allerdings wird die Befürchtung ausgesprochen, dass durch Festlegung oder gar Regulierung zu früh alternative Strukturen unterdrückt werden.

Empfehlung

Timingfrage klären. Handlungsfähigkeit der Bundesregierung gewährleisten, um bei zunehmendem Bedarf oder europäischen resp. internationalen Dynamiken schnell reagieren zu können.

Vorschlag für eine operationalisierbare Maßnahme

Etablierung einer ONS/Internet-der-Dinge/Dienste-„Watch" der Bundesregierung, die ein bis zwei Mal pro Jahr über aktuelle Entwicklungen berichtet und Handlungsbedarfe aufzeigt.

Befund

Vor allem Mittelständler, durchaus aber auch Führungskräfte in Großunternehmen, sind über die ONS-Thematik nicht bzw. nicht im Detail informiert und daher auch nicht für die Herausforderungen und mögliche Konsequenzen auf ihre Geschäftsprozesse sensibilisiert. Dadurch sind sie i. d. R. auch nicht in der Lage, ihre Interessen zu artikulieren resp. als „Lastenheft" einzubringen.

Empfehlung

Vor diesem Hintergrund der zu erwartenden zunehmenden Relevanz von ONS ist eine Informationskampagne zu allerersten anzuraten. Mittelständler wie Großunternehmen sollten über mögliche Standardisierungspläne aufgeklärt und über Kosten-/Nutzenaspekte der neuen Technologien informiert werden.

Vorschlag für eine operationalisierbare Maßnahme

In Zusammenarbeit mit Wissenschaft und Industrieverbänden (z. B. AIM, BITKOM, Informationsforum RFID etc.) sowie den betroffenen Branchenverbänden (z. B. GS1 Germany, VDA, VDMA etc.) und einschlägigen Forschungsprojekten (z. B. ADiWa, SemProM, Aletheia[26] und BRIDGE[27]) sollte eine Informationskampagne zum Internet der Dinge aufgesetzt werden.

Befund

Das Internet der Dinge unterliegt als Kommunikationsinfrastruktur gleichen Gefährdungs- und Missbrauchspotenzialen wie auch das gegenwärtige Internet mit seinen Entwicklungstrends hin zu Internet 2.0 oder Web 3.0.

Empfehlung

Missbrauchspotenziale, die durch die Identifizierbarkeit von Objekten und durch die damit erreichte Transparenz in Prozessen gegeben sind, sind zu minimieren.

[26] ADiWa (Allianz Digitaler Warenfluss; www.adiwa.net/), SemProM (Semantic Product Memory; www.semprom.org/) und Aletheia (Semantische Föderation umfassender Produktinformationen; www.aletheia-projekt.de/) sind im Rahmen von IKT2020 laufende BMBF-Forschungsvorhaben.

[27] BRIDGE (Building Radio Frequency IDentification for the Global Environment) ist ein EU-gefördertes „Integrated Project" mit dem Ziel, Barrieren bei der Implementation von RFID-Lösungen, basierend auf GS1 EPCglobal Standards, zu überwinden (siehe http://www.bridge-project.eu/; letzter Zugriff am 11.12.08).

Vorschlag für eine operationalisierbare Maßnahme

Vergabe von einschlägigen Forschungsprojekten, die insbesondere über die gegenwärtigen Arbeiten im BRIDGE-Projekt und bei EPCglobal hinausgehen und mittel- bis langfristige Fragestellungen des Internet der Dinge thematisieren.

Befund

Es ist zu wenig bekannt, für welche business cases überhaupt ein ONS erforderlich und sinnvoll ist.
Es ist noch unklar, welche Grundprinzipien (generische Bestandteile) einerseits notwendigerweise realisiert werden sollten und welche (branchen-)spezifischen Lösungen (individuelle Bestandteile) sich andererseits herausbilden werden.

Empfehlung

Förderung der Entwicklung beispielgebender Branchenlösungen. Diejenigen, die die meisten „showcases“ vorweisen können, werden auch die besten Ausgangspositionen beim Einbringen und Durchsetzen von Standards haben.

Vorschlag für eine operationalisierbare Maßnahme

First user action für die mittelständische Industrie.
Förderung von industriedominierten Verbundprojekten, in denen Wertschöpfungsketten prämiiert werden, die RFID/ONS erstmalig und von exemplarischer Bedeutung nachweisbar durchgehend einsetzen.

Befund

Erst wenn etwas Bewertbares vorliegt, wird sich die Industrie mit Ausnahme großer Handelsunternehmen dazu äußern. Es zeigt sich eine typische „Henne-Ei-Problematik“: Kaum einer will der first mover sein und auch nicht abstrakt an einer künftigen Infrastruktur mitarbeiten. Wenn ein Vorschlag auf dem Tisch liegt, wird man ihn prüfen und nutzen, ggf. verbessern oder aber ablehnen. Es besteht daher die Gefahr, dass sich Strukturen verfestigen, auf die deutsche Unternehmen keinen oder nur einseitig Einfluss genommen haben.

Empfehlung

Diskussion der Thematik im Dialogkreis RFID. Einbindung der entsprechenden Verbände erforderlich.

Vorschlag für eine operationalisierbare Maßnahme

Einbindung der Verbände in einschlägige Verbundprojekte sicherstellen.

Befund

Zu wenig Engagement deutscher Industrievertreter (insb. aus kleinen und mittelständischen Unternehmen) bei Standardisierungsdebatten und in entsprechenden Gremien. Arbeiten in Standardisierungsgremien findet selbst von Seiten großer Unternehmen nicht oder nicht regelmäßig oder gar in abgestimmter Weise statt. Die Präsenz bei Debatten auf europäischer Ebene ist entweder nicht oder nicht in der vollständigen Breite der deutschen Industriesektoren gegeben.

Empfehlung

Einbindung deutscher stakeholder in Standardisierungsgremien ermöglichen und Standardisierungsarbeiten flankieren und unterstützen. Einseitige Vertretung vermeiden und Agieren auf europäischer Ebene durch Mandatierung, z. B. durch den Dialogkreis RFID autorisieren.

Vorschlag für eine operationalisierbare Maßnahme

In FuE-Projekten Standardisierungsarbeitspakete stimulieren und in größerem Umfang (ggf. bis 100%) finanzieren. Den Dialogkreis RFID zu einer Dialogplattform „Internet der Dinge“ mit stringenter strategischer Ausrichtung weiterentwickeln.

Befund

Die Kosten-Nutzen-Asymmetrie bei RFID und im zu erwartenden Internet der Dinge hemmt eine Einführung über die Wertschöpfungskette, da bei Zulieferern in erster Linie Kosten entstehen, während nachgelagerte Bereiche der Wertschöpfungskette den Nutzen realisieren können.

Empfehlung

Die Verteilung der Kosten muss mit der Nutzung der Informationen gekoppelt werden. Zugleich muss dafür Sorge getragen werden, dass diese Informationen nur mit einer entsprechenden Berechtigung genutzt werden können, wenn dies notwendig erscheint. Einen Beitrag zu einer aufwandsgerechten Verteilung der Kosten könnte ein Modell für ein flächendeckendes Billingsystem leisten, das Lese-Ereignisse von RFID-Tags protokolliert und abrechnet, sowie eine Sperrung eines zu definierenden Teilnehmerkreises zulässt.

Vorschlag für eine operationalisierbare Maßnahme

Es ist gegenwärtig unsicher, ob hinsichtlich der Kosten-Nutzen-Asymmetrie bei RFID ein Marktversagen vorliegt oder in naher Zukunft droht. Wegen der potenziellen Schäden sollte im Gespräch mit den jeweiligen Branchen die Notwendigkeit einer staatlichen Moderation eruiert werden.

Befund

Die meisten Befragten erwarten, dass die Infrastruktur des Internet der Dinge wirtschafts- und technologiepolitisch neutral und nicht monopolisiert aufgesetzt wird.

Empfehlung

Es sollten rechtzeitig Strategien zur Umsetzung einer wirtschafts- und technologiepolitischen Neutralität und IT-Sicherheit beim ONS und dem Internet der Dinge erarbeitet werden. Das betrifft zum einen die internationale Abstimmung zur Neutralität des EPCglobal Networks, insbesondere innerhalb der Europäischen Union und mit den USA. Zum anderen sollte in Kooperation mit GS1 auf die unter Umständen notwendige nationale kartellrechtliche Absicherung des EPCglobal Networks hingearbeitet werden (GS1 ist ein kartellrechtlich anerkannter Rationalisierungsverband).

Vorschlag für eine operationalisierbare Maßnahme

Abstimmung der beteiligten Referate im Bundeswirtschaftsministeriums (etwa I B I Wettbewerbs-, Regulierungs- und Privatisierungspolitik, VII C I Grundsatzfragen der Informationsgesellschaft, IT-, Medien-, Kultur- und Kreativwirtschaft und VII C 3 Entwicklung Konvergenter IKT) und nachfolgende Gespräche mit GS1 im deutschen und internationalen Kontext.

Empfehlung allgemein

Eine fachliche Diskussion über RFID/ONS resp. Internet der Dinge sollte im Dialogkreis RFID geführt werden, der dazu um einige wichtige Mitglieder (z. B. aus angewandter Forschung) ergänzt werden sollte.

Vorschlag für eine operationalisierbare Maßnahme

ONS-Hearing bei nächster Sitzung des Dialogkreises oder Kamingespräch ONS: Uckelmann zu „Billing-Verfahren“, Prof. Boche zu „Kommunikationstechnologie“, Prof. Günther zu „ONS-Infrastruktur und -software“, Prof. Viola Schmid zu „Internetrecht/ RFID“ usw.

Literatur

[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]
Bundesministerium für Wirtschaft und Technologie (Hrsg.): RFID: Potenziale für Deutschland. Stand und Perspektiven von Anwendungen auf Basis der Radiofrequenz-Identifikation auf den nationalen und internationalen Märkten. Berlin 2007 [http://www.bmwi.de/ BMWi/Navigation/Service/ publikationen,did=200778.html].

[BMWi07b]
Bundesministerium für Wirtschaft und Technologie: European Policy Outlook RFID. Berlin, Juli 2007 [http://www.vdivde-it.de/Images/publikationen/ dokumente/RFID-Konf-E.pdf].

[BMWi08]
Bundesministerium für Wirtschaft und Technologie: 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/documents/roleofeuropeancommision/Reflections_on_ European_Policy_Outlook_RFID.pdf].

[BSI06]
Bundesamt für Sicherheit in der Informationstechnik: Risiken und Chancen des Einsatzes von RFID-Systemen. 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

Fragenkatalog Interview

B. Scholz-Reiter, Edt., Springer, 2008, pp. 183–197.
Ist Ihnen auf Basis unserer Einführung in die ONS-Thematik die Relevanz (für die deutsche Wirtschaft, für Ihr Unternehmen) deutlich geworden?

Sind die genannten fünf Problemfelder umfassend oder fehlen aus Ihrer Sicht wichtige Aspekte?

Unipolarität:

- Sehen Sie die jetzige, zentralisierte Infrastruktur für das Internet der Dinge als problematisch an? Was ist Ihr zentraler Kritikpunkt/Ihre zentrale Befürchtung?

- Welche Anforderungen richten Sie an die künftige Organisation der Infrastruktur?

- Wie bewerten Sie die Ansätze, nationale/regionale ONS-Roots zu errichten? Welche Probleme werden hierdurch gelöst, welche bleiben bestehen und welche kommen womöglich hinzu?

- Sehen Sie Alternativen hierzu?

- Welche Konsequenzen haben die Alternativen (im Vergleich mit dem bestehenden System) für Sie? Ist die potenzielle Abhängigkeit des Unternehmens von EPCglobal ein schwerwiegendes Argument gegen den Einsatz von ONS?

ONS-interne Vertrauens- und Machtstrukturen:

- Wer sollte aus Ihrer Sicht Zugriff auf welche Daten zu Produkten Ihres Unternehmens haben?

- Wie sind die Kontrollstrukturen zu errichten, damit ein sicherer und vertrauensbasierter Zugriff auf die Daten sichergestellt wird?

- Welche Lösungsmöglichkeiten gibt es im Rahmen eines Betreibermodells?

Integrität:

- Integrität und Authentizität der Daten sind sicherlich zwingend erforderlich. Welche Möglichkeiten sehen Sie, diese zu gewährleisten?

- Welche technischen und organisatorischen Lösungsoptionen kennen resp. präferieren Sie? Worin besteht der entscheidende Unterschied zur DNS-basierten Kommunikation und –Architektur aus Ihrer Sicht?

- Gibt es Ausnahmen, in denen auf höchste Anforderungen an Integrität verzichtet werden kann?

Verfügbarkeit:

- Sehen Sie die Verfügbarkeit und Funktionsfähigkeit des Internets der Dinge durch die gegenwärtige, zentrale ONS-Struktur als gefährdet an?

- Gibt es alternative Architekturen zu einigen wenigen (nationalen/regionalen) ONS-Roots, die die Verfügbarkeit der Daten und Ausfallsicherheit der Kommunikationswege besser gewährleisten können?

Vertraulichkeit und Anonymität:

- Welche Formen der Vertraulichkeit und Anonymität erscheinen Ihnen für Ihr Unternehmen besonders wichtig?

- Welche Rolle spielen für die Aufrechterhaltung von Vertraulichkeit und Anonymität technische Aspekte?

- Wie kann organisatorisch (z. B. durch Vergabe von Berechtigungen) im Internet der Dinge sichergestellt werden, dass kriminelle und Missbrauchspotenziale minimiert werden?

- Worin liegt eine mögliche Alternative zur ONS-basierten Kommunikation?

Wie würden Sie die genannten Problempotenziale gegeneinander gewichten? Was halten Sie für den prioritär zu behandelnden Problemkomplex?

Erwarten Sie durch die Nutzung eines derartigen Internet der Dinge organisatorische Veränderungen (Datenmodellierung, IT-Management, Ablauforganisation, Logistik, ...)? Worin liegen diese und wie bereiten Sie sich darauf vor?

Welche Voraussetzungen muss aus Ihrer Sicht eine künftige Infrastruktur mindestens erfüllen, damit Sie den Einstieg in das Internet der Dinge für Ihr Unternehmen befürworten?

Welche sicherheitstechnischen Anforderungen richten Sie an eine Infrastruktur und damit verbundene Services?

Wo sehen Sie bereits Lösungsansätze für sicherheitstechnische, datenschutzrechtliche Herausforderungen? Welche Fragen/Aspekte sind noch nicht oder völlig unzureichend adressiert?

In welchen Systemlösungen und in welchen Anwendungskonstellationen sind rechtliche (Haftungsrecht, Missbrauchsrecht etc.) Problemkomplexe und Fragestellungen im Besonderen zu erwarten?

Sind Ihnen Arbeiten bekannt (Gremienarbeiten, FuE-Projekte etc.), die die hier thematisierten Problempotenziale behandeln?

Welche Unterstützung wünschen Sie sich seitens der Öffentlichen Hand bei der Ausgestaltung der Infrastruktur und des flankierenden Sicherheitssystems zum Internet der Dinge? Sehen Sie hier überhaupt einen Regulierungsbedarf oder vertrauen Sie den Selbstregelungskräften des Marktes?

Sehen Sie bezogen auf Ihr Unternehmen / auf Ihre Klientel einen besonderen Unterstützungsbedarf?

Gesprächspartner

Interviewpartner	Funktion	Organisation	Branche
J. Bidlingsmaier	Project Manager Automotive	Seeburger AG	Automobilzulieferer Software
R. Glatz	Geschäftsführer Fachverband Software und Industrial Communication	VDMA e.V.	Maschinen- und Anlagenbau
W.-R. Hansen	Geschäftsführer	AIM-D e.V.	RFID-Verband
Dr. Sascha Henke	Unternehmensplanung	Robert Bosch GmbH, C/LP	Telemedizin / Medizintechnik
G. Leichert	Teamleiter Projekte Automotive	PSIpenta GmbH	Software- und Lösungsanbieter
G. Peeters	Geschäftsleitung Operations	CBR Fashion Holding GmbH	Textilindustrie Markenwaren
U. Quiede	RFID Project Manager	Kaufhof Warenhaus AG	Handel Warenhauskette
M. Scheferhoff	Program Manager RFID Lufthansa Technik Group	Lufthansa Technik Logistik GmbH	Logistik
D. Spannaus	IBM Managing Consultant, IBM Interactive	IBM Deutschland GmbH	Software- und Lösungsanbieter
M. Sprafke	Leiter Qualitätsplanung und Felddatenanalyse	Volkswagen AG	Automobilhersteller
R. Tröger	Projektleiter RFID	Gerry Weber International AG	Textilindustrie Markenwaren
D. Uckelmann	Wissenschaftler	Universität Bremen	Wissenschaft (Logistik)