A.1 RFID in Virtuellen Unternehmen: Potenziale von Data-on-Tag

Kerstin Werner, SAP Research CEC Dresden, 01187 Dresden
Eberhard Grummt, SAP Research CEC Dresden, 01187 Dresden und Technische Universität Dresden, Fakultät Informatik, Institut für Systemarchitektur, 01187 Dresden

1. Einleitung

Der Zusammenschluss verschiedener Firmen zu Virtuellen Unternehmen (*VU*) zum Erreichen gemeinsamer Ziele ist gegenwärtig ein sich deutlicher abzeichnender Trend, welcher auch den Bereich der Logistik betrifft. Hier begünstigen vor allem Anforderungen wie Kundenorientierung, kurze Lieferzeiten, geringe Reaktionszeiten auf Änderungen sowie möglichst geringe Kosten bei hoher Qualität diese Entwicklung. Die gemeinsame Nutzung global verteilter Dienste, Ressourcen, Informationen, Wissen aber auch die Verteilung von Risiken und Kosten stellt angesichts dessen häufig einen Vorteil gegenüber der vollständigen Alleinstellung dar. Durch den Einsatz der RFID-Technologie kann die Informationstransparenz innerhalb von Unternehmenskooperationen stark erhöht werden. Sie ermöglicht es, mit RFID-Transpondern (*Tags*) ausgestattete Trägerobjekte anhand eindeutiger Identifikationsdaten zu erkennen. Die Erkennung erfolgt über eine Funkverbindung zu Lesegeräten, welche die empfangenen Daten ggf. aufbereiten und an weiterverarbeitende Software übermitteln sowie üblicherweise auch Schreibfunktionalität für Tags besitzen [1]. Mit dem Einsatz von RFID geht die Frage nach Ort und Umfang der Datenhaltung einher. Es wird zwischen der Datenhaltung im Netzwerk *(Data-on-Network, DoN)* und der Datenhaltung auf Tags *(Data-on-Tag, DoT)* unterschieden, wobei ebenfalls hybride Ansätze existieren. Bisher befindet sich zumeist DoN im Einsatz. Bei diesem Ansatz werden lediglich Identifikationsdaten auf Transpondern gespeichert, die als Verweis auf weitere im Netzwerk gespeicherte Informationen über ein bestimmtes Objekt dienen. Der bevorzugte Einsatz dieses Verfahrens liegt unter anderem darin begründet, dass dafür bereits weit vorangetriebene Standardisierungsbemühungen existieren und vergleichsweise geringe Anforderungen an die zu verwendenden Tags gestellt werden müssen [2]. Bei dem Verfahren DoT werden alle relevanten Daten zu einem Trägerobjekt auf dem jeweiligen Transponder gespeichert. Im Gegensatz zu DoN wurde diesem Ansatz und dem darin enthaltenen Potenzial in Literatur und Praxis bisher weitaus weniger Beachtung geschenkt.

In diesem Beitrag wird gezeigt, dass durch die Verwendung von DoT spezifische Herausforderungen, welche beim Einsatz von RFID in VU bestehen, sehr gut erfüllt werden und dass dem Ansatz aus diesem Grund in Zukunft mehr Aufmerksamkeit entgegen

gebracht werden sollte. In Abschnitt 2 wird darauf eingegangen, welchen Nutzen die RFID-Technologie in VU erbringen kann und welche technische Infrastruktur von Unternehmen dafür bereitgestellt werden muss. Im Anschluss daran werden in Abschnitt 3 die beiden grundsätzlichen Ansätze zur Datenhaltung vorgestellt. In Abschnitt 4 wird beschrieben, welche speziellen Herausforderungen sich beim Einsatz von RFID in VU ergeben. Im Hinblick darauf werden anschließend in Abschnitt 5 die diesbezüglichen Potenziale von DoT aufgezeigt. Gleichzeitig wird in Abschnitt 6 auf vorhandene Nachteile und Beschränkungen des Ansatzes eingegangen. In Abschnitt 7 werden mit diesem Beitrag verwandte Arbeiten vorgestellt und abschließend in Abschnitt 8 eine Zusammenfassung sowie ein Ausblick auf zukünftige Arbeiten in diesem Gebiet gegeben.

2. Einsatz von RFID in Virtuellen Unternehmen

Der Einsatz der RFID-Technologie wird momentan verstärkt im Anwendungsbereich der Logistik vorangetrieben, weshalb sich in diesem Beitrag auf dessen Betrachtung beschränkt wird. Logistik befasst sich mit der Optimierung von Material- und Güterflüssen. Angesichts dessen besitzt die Technologie neben dem Potenzial zur Steigerung der Informationstransparenz innerhalb von Kooperationen viele weitere interessante Eigenschaften: Gegenüber dem Barcode bietet RFID Vorteile hinsichtlich der Auslesegeschwindigkeit, Speicherkapazität, Fälschungssicherheit, Wiederverwendbarkeit, Wiederbeschreibbarkeit und des entfernten Auslesens ohne Sichtverbindung [3]. Gleichzeitig können potenzielle Fehlerquellen wie Medienbrüche [4] eingeschränkt werden. Der verbreitete Einsatz der Technologie wird ebenfalls durch den Trend der Virtualisierung im Bereich der Logistik begünstigt. Die „Informationslücke“ zwischen realer und virtueller Welt soll stetig verkleinert werden. In diesem Zusammenhang finden häufig die Bezeichnungen „Echtzeit-Unternehmen“ und „Internet der Dinge“ Verwendung. Letzteres bezeichnet die Idee, dass Logistikgüter in Zukunft eine weltweit verfügbare digitale Entsprechung besitzen. Die RFID-Technologie ermöglicht es, den Waren- und Informationsfluss miteinander zu koppeln, indem auf Transpondern objektspezifische Daten einmalig gespeichert oder während seiner gesamten Lebenszeit mit Hilfe von Lesegeräten oder Sensoren gesammelt und aktualisiert werden [5]. Durch die gesteigerte Informationstransparenz innerhalb eines VU besteht darüber hinaus die Möglichkeit, effizient Tracking[1] und Tracing[2] von Objekten durchzuführen, die zwischen Partnerunternehmen ausgetauscht werden. Durch die Arbeit mit nahezu Echtzeitinformationen über Ort und Zustand von Objekten ist es möglich, schneller auf Planabweichungen und ver-

[1] Ermittlung des aktuellen Aufenthaltsortes eines Objektes

[2] Ermittlung der gesamten elektronischen Tracking-Historie eines Objektes

änderte Anforderungen zu reagieren, die Auslastung von Ressourcen besser zu planen und sogar Fälschungen zu erkennen [6]. Insgesamt ermöglicht der Einsatz von RFID innerhalb von VU im Bereich der Logistik potenziell eine gesteigerte Effizienz und Effektivität und damit letztendlich Kostenersparnisse. Eine Systeminfrastruktur, welche RFID-basierte Informationen verarbeitet, ist im Wesentlichen wie in Abbildung 1 dargestellt aufgebaut. Transponder werden von Lesegeräten der Sensorebene gelesen und ggf. beschrieben. Leseereignisse von Lesegeräten werden von Komponenten der Aufbereitungsebene gefiltert, aggregiert und semantisch angereichert („vorverarbeitet“). In der Persistenzebene werden sie anschließend gespeichert. Um einen Austausch vorhandener Informationen mit internen und externen Anwendungen zu ermöglichen, werden in der Austauschebene Abfrageschnittstellen bereitgestellt. Die Anwendungsebene beinhaltet darauf aufsetzende Anwendungen, welche zum Beispiel die Steuerung von Funktionalitäten unterer Ebenen sowie die Steuerung und Überwachung von Geschäftsprozessen beinhalten. Ein Datenaustausch findet unternehmensintern zwischen den in der Abbildung dargestellten Infrastrukturebenen sowie unternehmensübergreifend üblicherweise über die Austausch- und die Tag-Ebene statt.

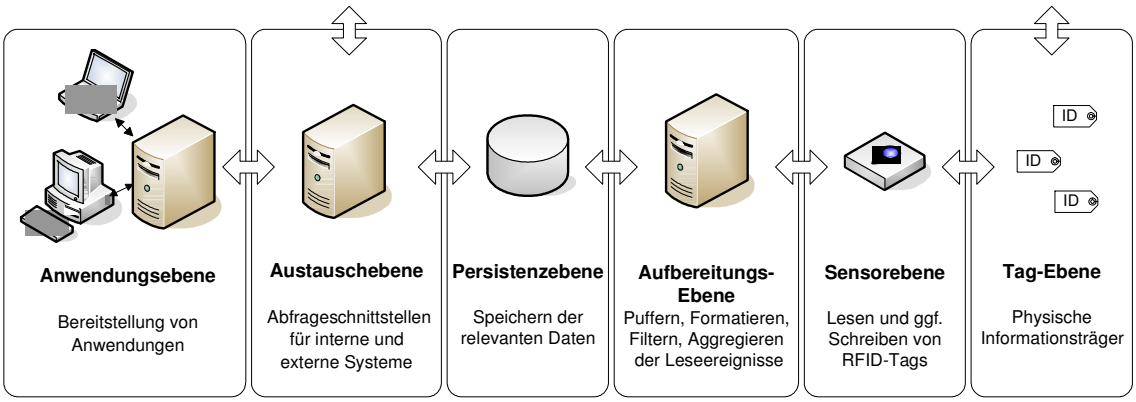

Abbildung 1: RFID-Infrastruktur: Bestandteile und deren Kommunikationsbeziehungen

3. Ansätze zur Datenhaltung

Bezüglich der Datenhaltung werden in RFID-Systemen die beiden Ansätze Data-on-Network und Data-on-Tag unterschieden. Beide werden in den folgenden Abschnitten hinsichtlich ihrer Funktionsweise und kennzeichnenden Eigenschaften vorgestellt.

3.1 Data-on-Network

Das Verfahren Data-on-Network (siehe Abbildung 2) zeichnet aus, dass alle mit einer bestimmten Tag-ID assoziierten Informationen zentral oder verteilt in einem Netzwerk gespeichert werden. Auf den eingesetzten Transpondern werden lediglich eindeutige Identifikationsnummern (z.B. *Electronic Product Codes, EPC*) gespeichert, die als Verweis auf die im Netzwerk gespeicherten Daten dienen.

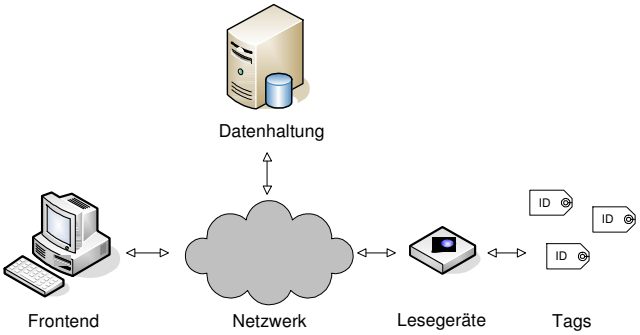

Abbildung 2: Funktionsweise von Data-on-Network

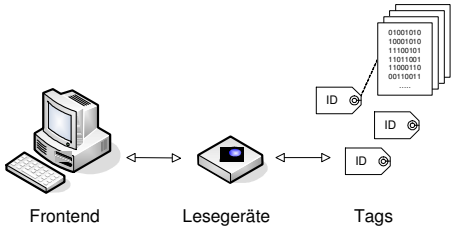

Abbildung 3: Funktionsweise von Data-on-Tag

Das beschriebene Prinzip liegt exakt den Bestrebungen von EPCglobal (http://www.epcglobalinc.org/) zu Grunde, wodurch die Standardisierungsbemühungen für dieses Verfahren im Bereich der Logistik bereits weit fortgeschritten sind. Zusätzlich können geringere Ansprüche an einzusetzende Transponder gestellt werden als bei dem Verfahren DoT. Alternativ zu Read-Write-Chips können WORM (Write Once Read Multiple)-Chips mit sehr geringem Speichervolumen zum Einsatz kommen, was sich positiv auf die dafür aufzubringenden Kosten auswirkt. Es ist allerdings zu beachten, dass die Verfügbarkeit der im Netzwerk befindlichen Informationen von dessen Funktionieren abhängig ist. Kennzeichnend für DoN ist, dass objektbezogene Daten im Netzwerk bei bestehendem Netzzugang unabhängig von der aktuellen physischen Verfügbarkeit eines entsprechenden Objektes, zeit- und ortsunabhängig verfügbar sind. Das Verfahren eignet sich also hauptsächlich dann, wenn gleichzeitige Zugriffe auf Informationen von verschiedenen Orten aus notwendig sind oder ein ständiges Abbild aktueller Objektdaten verfügbar sein muss.

3.2 Data-on-Tag

Neben Data-on-Network existiert das Verfahren Data-on-Tag (siehe Abbildung 3). Dieses verfolgt den Ansatz, zusätzlich zu Identifikationsdaten weitere relevante Daten, die über ein Objekt verfügbar sein sollen, auf dem jeweiligen Transponder zu speichern. Auf diese Weise befinden sie sich immer direkt am betreffenden Objekt und sind mit

ihm verfügbar. Ein Objekt kann so Daten über seine Identität, seinen Zustand, Qualitätsdaten, seine Vorgeschichte sowie seine geplante Zukunft mit sich führen. Aufgrund der potenziellen örtlichen Verteilung von Objekten und Daten wird dieser Ansatz häufig als eine Form der dezentralen Datenhaltung betrachtet. Bei der Nutzung des Verfahrens wird für die Speicherung objektbezogener Daten keine spezielle Netzwerkinfrastruktur benötigt. Es ist demzufolge unabhängig von einer solchen einsetzbar. Verwendete Lese- und Schreibgeräte der Sensorebene müssen allerdings über eine Benutzungsschnittstelle für ihre Steuerung verfügen. Abbildung 4 stellt den Zusammenhang zwischen benötigten Infrastrukturkomponenten und dem jeweiligen Ansatz zur Datenhaltung dar. Die Unabhängigkeit von bestimmten Infrastrukturbestandteilen macht DoT für Anwendungsgebiete interessant, in denen objektbezogene Informationen verfügbar sein sollen, aber kein zuverlässiger Zugriff auf eine entfernte Datenhaltung gegeben ist bzw. nur mit unverhältnismäßigem Aufwand realisierbar wäre, wie dies in virtuellen Ad-Hoc-Kooperationen häufig der Fall ist.

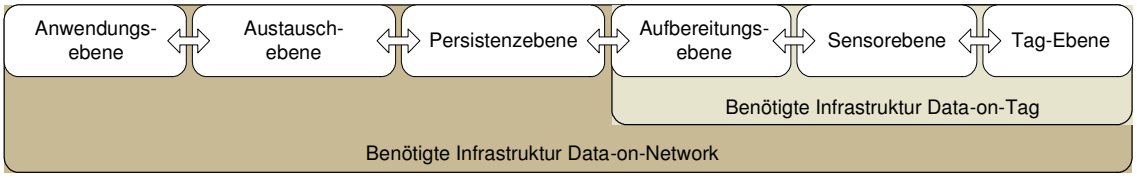

Abbildung 4: Benötigte Infrastrukturkomponenten für den Betrieb von Data-on-Network sowie Data-on-Tag

Sollen größere Datenmengen auf Transpondern gespeichert werden, impliziert dies erhöhte Anforderungen an die Hardware. Es muss beispielsweise dafür gesorgt werden, dass sie über genügend Speicherkapazität verfügen. Gleichzeitig müssen sie in den meisten Fällen wiederbeschreibbar sein, da Datenfelder vorhanden sein können, deren Inhalte aktualisiert werden müssen. Da je nach Anwendungsbereich die auf dem Tag zu speichernden Daten stark variieren können, sind Standardisierungen, wie beispielsweise Codierungsschemata, für das Verfahren DoT weitaus schwieriger durchzuführen als für Anwendungen, bei denen lediglich eine Identifikationsnummer auf den eingesetzten Transpondern stehen soll. Zusätzlich müssen geeignete Zugriffskontrollen auf Tag-Ebene eingesetzt werden, sofern kein übergreifendes Vertrauen zwischen allen an einer Lieferkette beteiligten Partner besteht.

4. Anforderungen an RFID-Lösungen beim Einsatz in VU

Für den Einsatz der RFID-Technologie in VU ergeben sich bestimmte Herausforderungen, welche durch spezifische in VU vorherrschende Anforderungen begründet sind. Das zeitlich begrenzte Bestehen eines Zusammenschlusses zwischen Unternehmen und die dynamische Zusammensetzung von Wertschöpfungsbeziehungen bewirken eine

häufige Reorganisation und Restrukturierung aufgrund permanenter Anpassungen an sich ändernde Anforderungen. Dieser dynamische Kontext erfordert für den Einsatz von RFID folgendes:

Flexibilität: Die Flexibilität innerhalb von VU betrifft organisatorische als auch technische Aspekte. Es variieren Kooperationsbeziehungen zwischen Partnern sowie ihre Rollen innerhalb des Zusammenschlusses. Gleichzeitig verändern sich RFID-basierte Daten, welche abhängig vom jeweiligen Kontext benötigt und gespeichert werden sowie daraus resultierend Änderungen hinsichtlich Vertrauensbeziehungen und zu vergebender Zugriffsrechte. Eine RFID-Lösung muss sich demzufolge schnell und einfach an sich ändernde Anforderungen anpassen lassen. Konfigurationsänderungen sollten unkompliziert und ohne großen Kostenaufwand durchzuführen sein.

Geringe Time-to-Operation: Die Nutzung der Technologie sollte möglichst wenig Zeit und Aufwand für die Bereitstellung und Integration von Infrastrukturkomponenten im Vorfeld erfordern. Diese Eigenschaft spielt zudem eine entscheidende Rolle im Hinblick auf die geforderte Flexibilität einer RFID-Lösung.

Geringe Kosten: Die für den Einsatz der Technologie aufzubringenden Kosten sollten möglichst gering und gerecht auf alle Partner verteilt sein. Sie setzen sich aus den Komponenten Hardware-, Software-, Integrations- sowie Betriebs- und Wartungskosten zusammen. Speziell für RFID-Tags werden die Hardwarekosten durch Betriebseigenschaften, wie Frequenzbereich, Energieversorgung, Bauform und verwendete Speichertechnologie beeinflusst, die abhängig vom jeweiligen Anwendungsbereich gewählt werden müssen.

Kompatibilität: Angesichts variabler Kooperationsbeziehungen sollte die Interoperabilität zwischen bestehenden Systemlandschaften verschiedener Partner erhöht werden. Auf diese Weise können große Integrationsaufwendungen, welche beispielsweise durch inkompatible Kommunikationsinfrastrukturen oder Datenformate bestehen, vermindert werden. Diese Anforderung wird durch aktuelle Standardisierungsbemühungen adressiert. Für kollaborative RFID-basierte Anwendungen sind vor allem die zwei Gremien EPCglobal und ISO (International Organization for Standardization) (http://www.iso.org/iso/en/ISOOnline.frontpage) tätig. Weitere Herausforderungen für den Einsatz der Technologie entstehen dadurch, dass in VU Wissen unter den Partnern geteilt werden soll, um schneller auf sich ändernde Anforderungen reagieren zu können. Die durch die Technologie gesteigerte Informationstransparenz sowie die gemeinsame Nutzung und Verarbeitung von Informationen verlangt diesbezüglich die Einhaltung folgender Aspekte:

Gewährleistung von Datensicherheit: Um die Potenziale von RFID zu nutzen, muss Datensicherheit bei einem Einsatz der Technologie in VU ganzheitlich gewährleistet

werden. Dies beinhaltet den Schutz von inner- und überbetrieblichen Datenflüssen. Diese finden auf Ebene der Transponder statt sowie zwischen Informationssystemen der beteiligten Kooperationspartner, aber auch zwischen Kooperationspartnern und Services externer Dienstleister wie Zertifizierungsstellen und Auffindungsdiensten [7].

Gewährleistung von Datenschutz: Bislang wurde die Gefahr der mangelnden Gewährleistung des Datenschutzes beim Einsatz der RFID-Technologie hauptsächlich von Verbraucherschützern kritisiert [8,9,10]. Es besteht die Befürchtung, dass personenbezogene Profile über Bewegungen, soziale Beziehungen oder Kaufverhalten aufgestellt werden. Diese können durch die Speicherung, Verknüpfung und Auswertung RFID-basierter Daten erstellt werden, sofern Verbraucher getaggte Objekte besitzen und mit diesen assoziiert werden können. Aus der Sicht von Unternehmen sind diese Befürchtungen bedeutsam, da eine mangelnde Akzeptanz durch Verbraucher den übergreifenden Einsatz der RFID-Technologie behindern kann. Aufgedeckte Verstöße gegen Datenschutzregelungen können die Reputation von Unternehmen negativ beeinflussen.

5. Potenziale von Data-on-Tag

In Abschnitt 5 wurden spezifische Herausforderungen genannt, die beim Einsatz der RFID-Technologie in VU berücksichtigt werden sollten. In diesem Abschnitt werden nun Argumente angeführt, die zeigen, dass der Ansatz DoT im Hinblick darauf vielversprechende Vorteile aufweist. Viele davon lassen sich auf die in Abbildung 4 dargestellte Unabhängigkeit von einigen Infrastrukturkomponenten zurückführen.

5.1 Flexibilität und geringe Time-to-Operation

In Szenarien, in denen sich die Struktur von Lieferbeziehungen häufig ändert, kann Geld und Zeit gespart werden, indem der Aufwand für die Einrichtung benötigter Infrastruktur minimiert wird. RFID-Lösungen, die DoT umsetzen, können zeitnah zum Einsatz kommen, da sie unabhängig von einigen Infrastrukturbestandteilen einsetzbar sind. Hat ein Hersteller beispielsweise häufig wechselnde Zulieferer, müssen zu Beginn einer Kooperation lediglich die benötigten Tags bereitgestellt werden. Lesegeräte können für den Zeitraum einer Kooperation verliehen werden. So können Investitionen geringer ausfallen und der Aufwand für die Einrichtung komplexer Zugriffskontrollen auf Infrastrukturebenen wird dezimiert.

5.2 Geringere Infrastrukturkosten

Wie unter Abschnitt 5.1 bereits angedeutet wurde, können durch den Einsatz von DoT erhebliche Kosten eingespart werden, da auf das Vorhandensein bestimmter Infrastrukturbestandteile verzichtet werden kann. Neben den Kosten für die Beschaffung entfallen

gleichzeitig Kosten für die Integration und Wartung bestehender Bestandteile. Dieser Aspekt fällt vor allem dann ins Gewicht, wenn für die Laufzeit einer Kooperation beschaffte Komponenten in einer späteren Kooperation mit anderen Partnern inkompatibel sind und kostspielig erneuert oder angepasst werden müssten.

5.3 Einschränkung von Kompatibilitätsproblemen

Der Datenhaltungsansatz DoT beinhaltet hinsichtlich der Kompatibilität von Infrastrukturbestandteilen geringere Anforderungen als DoN. Viele Unternehmen besitzen bereits proprietäre interne RFID-Lösungen. Die vorhandene Infrastruktur kann ohne Anpassungen weiterhin genutzt werden, da der Austausch RFID-basierter Daten ausschließlich auf Tag-Ebene stattfindet. Unternehmensübergreifende Kompatibilität muss lediglich auf dieser und auf Sensorebene gewährleistet sein. So müssen beispielsweise einheitliche Datenformate und Übertragungsfrequenzen innerhalb eines Kooperationszusammenschlusses gewählt werden.

5.4 Datensicherheit

DoT ermöglicht einen objekt-bezogenen asynchronen Austausch von Informationen zwischen Kooperationspartnern. Einfache Zugriffsrechte lassen sich bereits durch die Notwendigkeit des physischen Zugriffs auf die getaggten Objekte umsetzen. Neben diesem Vorteil bietet DoT eine verbesserte Verfügbarkeit durch lokal vorhandene Informationen, die direkt am Objekt unabhängig vom Funktionieren oder Engpässen einer Netzwerkinfrastruktur zugänglich sind.

5.5 Datenschutz – Vorteil für Verbraucher

Der Ansatz DoT bietet neben den Vorteilen für Unternehmen auch Nutzen für Verbraucher. Im Vergleich zu DoN birgt er Vorteile hinsichtlich der Gewährleistung von Datenschutz, insbesondere von *location privacy* und *data privacy* [3]. Indem Daten nicht zentral in einem Netzwerk gespeichert werden, wird ihre Verknüpfung, Auswertung und Verbreitung stark erschwert. Gleichzeitig bietet der Ansatz Möglichkeiten, dem Nutzer eine gesteigerte Kontrolle über RFID-bezogene Daten zu ermöglichen, indem er sie in seinem Besitz persönlich verwalten kann. Mit der Einschränkung der Bedrohung des Datenschutzes durch die RFID-Technologie kann die Akzeptanz von Verbrauchern stark gefördert werden. Somit hat der beschriebene Vorteil von DoT ebenfalls einen Nutzen für Unternehmen.

6. Nachteile bzw. Beschränkungen des Ansatzes

Die ausschließliche Speicherung und lokale Verfügbarkeit RFID-basierter Daten impliziert neben den unter Abschnitt 5 beschriebenen Vorteilen gleichzeitig einige Nachteile, auf welche in diesem Abschnitt eingegangen wird.

6.1 Hohe Kosten für Tags

Für den Einsatz von DoT werden zumeist RFID-Transponder mit einer größeren Speicherkapazität als vergleichsweise für den Einsatz von DoN benötigt. Einfache WORM-Chips reichen häufig nicht aus. Auf Tags gespeicherte Daten müssen während des Lebenszyklus' eines Objektes verändert und aktualisiert werden, was die Nutzung von Read-Write-Chips erfordert. Die exklusive Datenhaltung auf Transpondern verlagert die Bedrohung der Vertraulichkeit gespeicherter Informationen auf die Tag-Ebene. Aus diesem Grund müssen dort bei Bedarf entsprechende Mechanismen zur Gewährleistung von Zugriffskontrollen oder Verschlüsselung umgesetzt werden. Die genannten Faktoren tragen dazu bei, dass im Gegensatz zum Ansatz DoN bei DoT deutlich höhere Kosten für Transponder anfallen. Es ist allerdings der stetige Trend zu verzeichnen, dass die Technologiekosten sinken, so dass die unter Abschnitt 5 angeführten Vorteile von DoT die dafür erforderlichen Investitionen leicht ausgleichen können. Des Weiteren können wiederbeschreibbare Tags häufig wiederverwendet werden.

6.2 Mangelnde Standardisierung

Im Kontext Virtueller Unternehmen muss der Einsatz der RFID-Technologie flexibel möglich sein und auf sich ändernde Anforderungen muss zeitnah reagiert werden können. Inkompatibilitäten zwischen verwendeten Datenformaten oder Systeminfrastrukturen verschiedener Kooperationspartner stellen in dieser Hinsicht ein Hemmnis dar. Momentan werden diesbezügliche Standardisierungsbemühungen hauptsächlich für den Ansatz DoN vorangetrieben [11]. Das kann darauf zurückgeführt werden, dass auf Tags gespeicherte Daten je nach Anwendungsgebiet und Kontext, wie bestehende Vertrauens- und Abhängigkeitsverhältnisse der Partner sowie technische Rahmenbedingungen, variieren. Dieser Trend könnte allerdings beeinflusst werden, wenn den Potenzialen des DoT-Ansatzes eine größere theoretische und praktische Beachtung von Seiten der Forschung und der Industrie entgegengebracht würde. Eine breitere Unterstützung des Ansatzes durch Standards würde sich gleichzeitig positiv auf die unter Abschnitt 6.1 begründeten relativ hohen aufzubringenden Kosten auswirken. Eine Möglichkeit, branchenspezifische Anforderungen zu berücksichtigen wäre, Daten in Form eines selbstbeschreibenden, erweiterbaren und gegebenenfalls komprimierten XML-Formats auf Tags

zu speichern. Sofern genügend Speicherplatz verfügbar ist, könnte dies einen Lösungsansatz der genannten Probleme hinsichtlich der Standardisierung darstellen.

6.3 Datensicherheit auf Tag-Ebene

Die Speicherung von potenziell vertraulichen Informationen auf Transpondern verlagert den Angriffspunkt von der Netzwerkinfrastruktur und den eingesetzten Datenbanken auf die Tags selbst. Ihre physische Verteilung und die Notwendigkeit der räumlichen Nähe zum Erlangen von Informationen kann ein Plus an Sicherheit darstellen. Gleichzeitig ist es jedoch Angreifern, die physische Kontrolle über Transponder erhalten, prinzipiell möglich, durch mehr oder weniger aufwändige Analyse der Hardware und ihres Verhaltens Informationen zu extrahieren. (Derartige "Probing"- und "Side-Channel"-Attacken wurden insbesondere in Bezug auf Smartcards bekannt). Insbesondere wenn die Sicherheit ausschließlich auf dem Geheimhalten von auf Tags, z.B. in speziell geschützten Bereichen gespeicherten Informationen wie Schlüssel, Algorithmen oder Hardware-Designs gründet, ist es für Angreifer nur eine Aufwandsfrage, diese Geheimnisse in Erfahrung zu bringen und damit die Sicherheit zu brechen. Entsprechend sollten Informationen auf Transpondern verschlüsselt abgelegt und die Dechiffrierschlüssel nicht ausschließlich auf den Tags gespeichert werden. Insbesondere in VU mit mehreren Teilnehmern ist es wünschenswert, Zugriffsrechte nicht nur auf den gesamten Tag-Speicher zu vergeben bzw. zu unterbinden, sondern diese auf bestimmte Speicherbereiche und Operationen, ggf. auch zeitlich begrenzt, einzuschränken. Dies stellt erhöhte Anforderungen an die Hardware und erhöht dadurch die Kosten, außerdem wirft es Fragen bezüglich der Schlüsselverteilung auf. Diese könnte fälschungssichere Lesegeräte sowie einen Netzwerkzugang erfordern, was zu hybriden Systemdesigns führen würde.

7. Verwandte Arbeiten

Neben dieser Arbeit existieren bereits weitere Beiträge, welche die Aussage vertreten, dass der Ansatz DoT ein vielseitiges Potenzial birgt, welches in Literatur und Forschung bisher ungenügend beleuchtet und untersucht wurde. In [12] wird beispielsweise ein eher wirtschaftlich fokussierter Vergleich der beiden Ansätze zur Datenhaltung vorgenommen, um letztendlich vor allem Vorteile von DoT sowie hybrider Ansätze zu verdeutlichen. In [13] werden hingegen hauptsächlich Datenschutzaspekte und mit dem Einsatz der RFID-Technologie verbundene Verbraucherängste adressiert. DoT wird in diesem Zusammenhang als eine datenschutzfreundliche Einsatzmöglichkeit der Technologie vorgestellt, die Vorteile für Verbraucher sowie Unternehmen bietet.

8. Zusammenfassung und Ausblick

In diesem Beitrag wurde erläutert, wie die RFID-Technologie insbesondere dann für VU im Logistik-Umfeld gewinnbringend eingesetzt werden kann, wenn relevante Daten direkt auf Transpondern gespeichert werden. Dieser Data-on-Tag genannte Ansatz grenzt sich gegenüber Data-on-Network insofern positiv ab, dass durch die Vermeidung einer Datenhaltung im Netzwerk die Informationen direkt am Objekt verfügbar sind. Die Systemkosten können durch Verzicht auf einige in DoN-Szenarien benötigte Infrastrukturkomponenten verringert werden. Die Verwendung von mobilen RFID-Lesegeräten und leichtgewichtigen Steuerungseinheiten ermöglicht die flexible Bildung und Auflösung von für temporäre Unternehmenskooperationen notwendigen Infrastrukturen. Probleme der logischen Zugriffskontrolle werden in einfachen Szenarien auf die Beschränkung des physischen Zugriffs abgebildet. Sollen hingegen mehrere Parteien unterschiedliche Lese- und Schreibrechte auf gemeinsam genutzte Tags erhalten, steigen die technischen Anforderungen an die Hardware und damit die Kosten. Insbesondere die Standardisierung entsprechender Transponder stellt ein Hindernis für den problemlosen Einsatz dar. Der Verzicht auf eine zentrale Speicherung von RFID-basiert erfassten Informationen entspricht außerdem einer wesentlichen Forderung von Datenschützern, da solche Informationen in Verbindung mit persönlichen Daten leicht kombiniert und missbraucht werden können. Einen zukünftigen Forschungsgegenstand stellt die Frage dar, inwiefern hybride Systemkonzepte die Vorteile der Ansätze DoT und DoN vereinen können und wie Anforderungen von Industrie und Konsumenten balanciert berücksichtigt werden können. Durch DoT entstehen hohe Anforderungen an die Bereitstellung geeigneter Zugriffskontrollmechanismen auf Tag-Ebene, deren Untersuchung und Weiterentwicklung es bedarf. Viele Anwendungsmöglichkeiten für DoT setzen den Einsatz wiederbeschreibbarer Tags voraus. Dies erfordert die Verbesserung und Anpassung bestehender Eingabekontrollen und Filtermechanismen auf der Ebene von Lesegeräten sowie verwendeter Middleware, da ansonsten über wiederbeschreibbare Tags Viren oder Fehlinformationen in Systeme infiltriert werden könnten [14].

9. Literatur

[1] AIM Inc. RFID - A basic primer. http://www.aimglobal.org/technologies/rfid/resources/RFIDPrimer.pdf, August 2001.

[2] Ken Traub, Greg Allgair, Henri Barthel, Leo Burstein, John Garrett, Bernie Hogan, Bryan Rodrigues, Sanjay Sarma, Johannes Schmidt, Chuck Schramek, Roger Stewart, and KK Suen. The EPCglobal Architecture Framework - EPCglobal Fi-

nal Version of 1 July 2005. http://www.epcglobalinc.org/standards/Final-epcglobalarch-20050701.pdf, Juli 2005.

[3] Bundesamt für Sicherheit in der Informationstechnik. Risiken und Chancen des Einsatzes von RFID-Systemen (rikcha) - Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf, 2005.

[4] Elgar Fleisch und Friedemann Mattern. Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis. Springer-Verlag, Berlin, Heidelberg, 2005.

[5] 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, März 2007.

[6] Ari Juels. Strengthening EPC tags against cloning. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pages 67-76, New York, USA, 2005. ACM Press.

[7] Eberhard Grummt, Kerstin Werner, and Ralf Ackermann. Sicherheitsanalyse in RFID-basierten Wertschöpfungsnetzen. In D-A-CH Security, 2007.

[8] Katherine Albrecht. Supermarket Cards: The Tip of the Retail Surveillance Iceberg. Denver University Law Review, 79:534-539 and 558-565, 2002.

[9] Oliver Berthold, Oliver Günther, and Sarah Spiekermann. RFID: Verbraucherängste und Verbraucherschutz. Wirtschaftsinformatik, S. 1-9, 2005.

[10] Oliver Günther and Sarah Spiekermann. RFID and the perception of control: the consumer's view. Commun. ACM, 48(9):73-76, September 2005.

[11] Tsukada Mitsuo. Recent Activities for RFID Standardization. NTT Tech Rev, 4(1):56-60, 2006.

[12] Thomas Diekmann, Adam Melski, and Matthias Schumann. Data-on-Network vs. Data-on-Tag: Managing Data in Complex RFID Environments. hicss, 0:224a, 2007.

[13] Kerstin Werner, Eberhard Grummt, Stephan Groß, Ralf Ackermann: Data-on-Tag: Approaches to Privacy-friendly Usage of RFID Technologies. 3rd European Workshop on RFID Systems and Technologies, 12.06.2007.

[14] Melanie Rieback, Patrick N. D. Simpson, Bruno Crispo, Andrew S. Tanenbaum: RFID Malware: Design Principles and Examples. In: Pervasive and Mobile Computing (PMC) Journal 2 (2006), S. 405–426