

RFID-Technologie: Verbesserung des Datenschutzes durch Nutzung des technischen Gestaltungsspielraums

Dirk Henrici, Tino Fleuren
Technische Universität Kaiserslautern
Gottlieb-Daimler-Straße
67663 Kaiserslautern
henrici@informatik.uni-kl.de

Zusammenfassung

RFID-Transponder dienen primär der eindeutigen Identifikation von Objekten, z.B. von Waren, Behältern oder Dokumenten. Weitergehend möchte man den Objekten eine Vielzahl von Daten zuordnen, die das Objekt beschreiben, seine Historie dokumentieren oder es in den Kontext anderer Objekte stellen. In diesem Beitrag wird dargestellt, welche technischen Gestaltungsspielräume es zur Speicherung derartiger Daten gibt und welche Auswirkungen bezüglich Kosten, Flexibilität und Datenschutz die Wahl des Speicherortes hat. Dadurch soll erreicht werden, dass diesbezügliche Designentscheidungen nicht unüberlegt oder mit einseitiger Sichtweise getroffen werden. Dieser Beitrag bezieht sich nur auf Transponder, die als reiner Datenspeicher genutzt werden. Transponder mit Prozessor, kryptographischer Hardware oder Sensoren bedürfen zum Teil einer gesonderten Betrachtung.

1 Gestaltungsspielräume

Grundsätzlich gibt es zwei mögliche Speicherorte für zu einem Objekt gehörige Daten: Der Transponder selbst und Datenbanken im Hintergrund, d.h. im sogenannten Backend. Dies ist in Abbildung 1 dargestellt.

Welche Daten wo gespeichert werden, stellt einen Gestaltungsspielraum für die technische Implementierung dar. Bezüglich der Anwendungsmöglichkeiten ist der Speicherort inzwischen praktisch unerheblich. Die Wahl schränkt die Möglichkeiten somit nicht ein. Jedoch kann die Implementierung grundlegende Unterschiede aufweisen, die sich auf Randbedingungen wie Kosten, Flexibilität und Datenschutz auswirken.

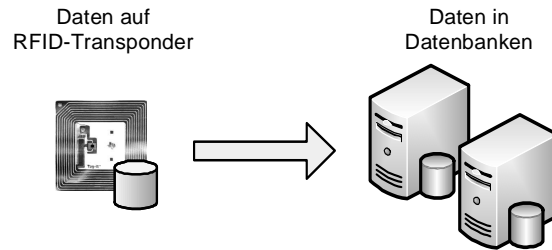


Abbildung 1: Daten im Transponder und in Datenbanken im Backend

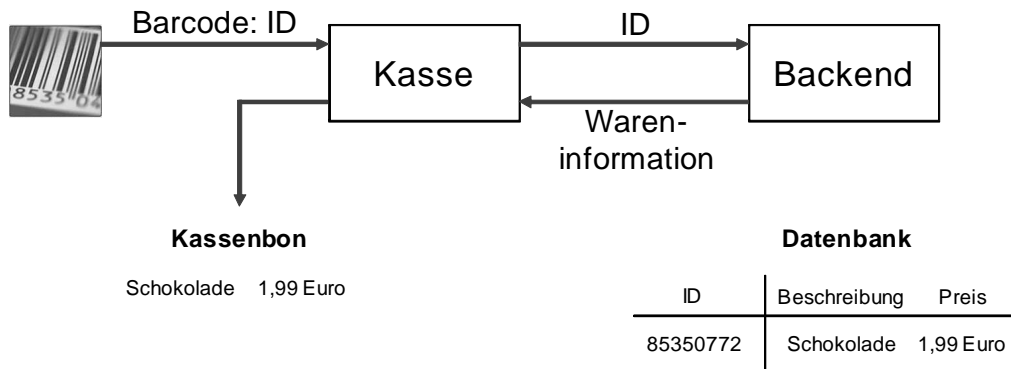


Abbildung 2: Zusammenspiel von Barcode und Backend im Supermarkt

Bei optischen Barcodes hatte man vielfach kaum eine Wahl, da die Speicherkapazität bei ein-dimensionalen Codes sehr begrenzt ist. So umfasst der bekannte EAN-Code (European Article Number) nur 13 Ziffern. Dies reicht nicht aus, um Waren eindeutig zu identifizieren oder gar noch weitere Daten zu hinterlegen, sodass dieser Code nur jeweils eine Kennung für den Hersteller und das Produkt enthält. Alle weiteren Daten müssen somit im Backend gespeichert werden.

Ein Anwendungsbeispiel ist in Abbildung 2 dargestellt. In diesem Supermarkt-Szenario enthält der Barcode eine Kennung für Hersteller und Produkt. In der Abbildung ist sie als „ID“ eingezeichnet. In Datenbanken im Backend werden jeder Kennung zusätzliche Informationen zugeordnet, beispielsweise eine Produktbeschreibung und der aktuelle Verkaufspreis. Der Ablauf ist dann wie folgt: An der Kasse wird der Barcode eines Produktes gescannt. Mit der gelesenen Kennung kann nun die benötigte Wareninformation aus dem Backend abgefragt werden. Für die Kasse ist die Information danach genauso verfügbar, als sei sie direkt vom Barcode gelesen worden.

In den folgenden Abschnitten dieses Kapitels wird der Gestaltungsspielraum für die Aufteilung der zu speichernden Daten zwischen Transponder und Backend beschrieben, ohne eine Wertung vorzunehmen. In Kapitel 2 werden die Auswirkungen der unterschiedlichen Aufteilungen diskutiert und darauf basierend im Kapitel 3 eine Empfehlung gegeben, für welche Aufteilung man sich in der Praxis entscheiden sollte.

1.1 Praxisrelevante Aufteilungen

In den folgenden Abschnitten wird dargestellt, welche unterschiedlichen Mengen an Daten auf Transpondern gespeichert werden können. Die anderen benötigten Daten werden jeweils im Backend vorgehalten. Die Darstellung ist abstrakt gehalten. Im Unterkapitel 1.2 werden daher für unterschiedliche Anwendungsszenarien praktische Beispiele gegeben.

Transponder mit Identifier und umfangreichen Daten

In diesem Szenario werden umfangreiche Daten, z.B. Produktinformationen, direkt auf den Transpondern gespeichert. Das hier verfolgte Prinzip ist, alle ein Objekt beschreibenden Daten direkt im RFID-Transponder, der am Objekt angebracht ist, vorzuhalten. Über einen weltweit eindeutigen Identifier kann das Objekt identifiziert werden. Die Speicherung noch weiterer Daten im Backend wäre damit möglich, wird hier jedoch nicht weiter betrachtet.

Transponder mit Identifier und wenigen Zusatzdaten

Auch diesem Szenario werden auf dem Transponder Daten gespeichert, die das Objekt eindeutig identifizieren. Diese Daten sind im Regelfall strukturiert, d.h. der Identifier ist in mehrere Teile untergliedert. Über diese das Objekt eindeutig identifizierende Daten können weitere Daten, die im Backend gespeichert werden, dem Objekt zugeordnet werden.

Über diese Daten zur Identifikation hinaus, werden in diesem Szenario einige wenige zusätzliche Daten direkt auf dem Transponder gespeichert. Dabei handelt es sich im Regelfall um Daten, die für den Lebenszyklus des Objekts eine besondere Bedeutung besitzen.

Transponder mit mehrfach strukturiertem Identifier

In diesem Szenario werden auf dem Transponder ausschließlich Daten gespeichert, die notwendig sind, um ein Objekt eindeutig zu identifizieren. Damit können dem Objekt im Backend beliebige weitere Daten zugeordnet werden.

Die Daten, die das Objekt identifizieren, besitzen eine Struktur. Das bedeutet, dass das Datenwort sich in mehrere Teile untergliedert, wobei jedes Teil eine eigene Bedeutung hat.

Als Beispiel sei hier die Nachfolgeversion des EAN-Codes für den Handel genannt: In einer Form des Electronic Product Code (EPC) werden hier Hersteller, Produkttyp und eine Seriennummer gespeichert. Zusammengenommen kann damit ein Objekt weltweit eindeutig identifiziert werden. Das Datenwort hat dabei eine dreiteilige Struktur, wobei die Einzelteile jeweils eine interpretierbare Bedeutung besitzen.

Transponder mit minimal strukturiertem Identifier mit Anwendungsbezug

Ähnlich wie im vorangegangenen Szenario werden auch hier auf dem Transponder ausschließlich Daten gespeichert, die notwendig sind, um ein Objekt eindeutig zu identifizieren. Der Unterschied hier ist, dass die Struktur des Datenworts auf das technisch notwendige Mindestmaß reduziert wird. Die Struktur hat dabei einen Bezug zur jeweiligen Anwendung.

Das genannte Mindestmaß besteht aus zwei Teilen: Ein erster Teil, der angibt, wer für den Transponder zuständig ist, und ein zweiter Teil, der den Identifier eindeutig macht. Der erste Teil könnte etwa den Hersteller des Produktes bezeichnen. Die Strukturierung verhilft zu Skalierbarkeit, da die Zuständigkeiten und damit Last unter Nutzung des ersten Identifier-Teils auf unterschiedliche Backendsysteme verteilt werden können.

Transponder mit minimal strukturiertem Identifier ohne Anwendungsbezug

Dieses Szenario entspricht dem vorher beschriebenen, jedoch lassen die einzelnen Teile des Identifiers keinen Rückschluss auf die Anwendung oder irgendwelche Eigenschaften des Objektes zu.

Der Identifier besteht hier aus zwei Teilen: Der erste Teil gibt die verwaltende Stelle an, die keinen Bezug zum mit dem jeweiligen RFID-Tag ausgestatteten Objekt haben sollte, also weder den Hersteller, noch Besitzer oder Eigentümer bezeichnen. Der zweite Teil ist auch hier wieder eine Seriennummer, die das Objekt innerhalb der verwaltenden Stelle eindeutig bezeichnet. Auch hier dient die Struktur der Skalierbarkeit, doch geben die Bestandteile des Identifiers keine Informationen über das jeweilige Objekt preis.

Transponder mit strukturlosem Identifier

In diesem Szenario speichert ein Transponder ausschließlich eine zufällig wirkende Seriennummer. Dies ist ausreichend, um in geschlossenen Systemen weitere Daten aus dem Backend dem jeweiligen Objekt zuzuordnen.

In organisationsübergreifenden RFID-Systemen sind Transponder mit strukturlosem Identifier nicht sinnvoll einsetzbar, da das auslesende Unternehmen nicht erfährt, welches andere Unternehmen es zum Erhalten weiterer Informationen kontaktieren muss. Die Skalierbarkeit des Systems ist damit stark eingeschränkt. Über Pseudonymisierungsinfrastrukturen lässt sich dieses Problem theoretisch umschiffen. Aufgrund einiger sich ergebender Nachteile ist diese Option für die Praxis derzeit jedoch kaum interessant [Hen2008], sodass der Einsatz strukturloser Identifier nur in geschlossenen Systemen zweckmäßig ist.

Transponder mit wechselndem Identifier

Transponder mit einem statischen Identifier können dazu benutzt werden, Objekte wieder zu erkennen und damit Bewegungsprofile zu erstellen. Unter Benutzung vernetzter Lesegeräte können Objekte auch verfolgt werden. Diese Charakteristika sind oftmals gewünscht, beispielsweise in der Logistik, stellen jedoch beim Endverbraucher ein Problem für die Privatsphäre dar, da somit indirekt auch Personen wieder erkannt und verfolgt werden können. Mit sich regelmäßig ändernden Identifiern kann dafür gesorgt werden, dass nur Berechtigte Objekte wieder erkennen und verfolgen können und so die Privatsphäre geschützt wird.

Die notwendigen Verfahren sind Forschungsgegenstand, auch in der Arbeitsgruppe der Autoren (AG ICSY an der TU Kaiserslautern). Zur sicheren Implementierung werden jedoch Transponder benötigt, die nicht nur Daten speichern können, sondern auch noch eine Zusatzfunktionalität besitzen. Da Transponder mit derartiger Zusatzfunktionalität nicht Gegenstand

	Identifizier und umfangreiche Daten	Mehrfach strukturierter Identifier	Minimal-Identifier mit Anwendungsbezug	Minimal-Identifier ohne Anwendungsbezug
Kennung des Herstellers	X	X	X	X
Kennung des Produktmodells	X	X	X	X
Seriennummer zum Eindeutigmachen	X	X	X	X
Herstellungsdatum	X	X		
Mindesthaltbarkeitsdatum	X	X		
Hersteller im Klartext	X			
Produktmodell im Klartext	X			
Deklaration der Inhaltsstoffe	X			
Unverbindliche Preisempfehlung	X			
Gebrauchsanweisung	X			
Identifier der verwaltenden Stelle				X
Eindeutige Nummer innerhalb der verwaltenden Stelle				X

Abbildung 3: Praxisbeispiel: Supermarktartikel

dieses Beitrags sind, werden wechselnde Identifier nicht weiter betrachtet, sollten aber in dieser Auflistung der Vollständigkeit halber erwähnt werden.

1.2 Praxisbeispiele

Im Folgenden wird an einer Reihe von praktischen Beispielen gezeigt, wie sich die Nutzung unterschiedlicher Aufteilungen auswirkt. Die Beispiele sind alle auf organisationsübergreifende RFID-Systeme ausgerichtet. In geschlossenen Systemen wären auch Transponder mit strukturlosem Identifier eine interessante Option.

Zu jedem Beispiel gibt es eine Tabelle, in der für die unterschiedlichen Aufteilungen dargestellt wird, welche Daten direkt auf den RFID-Transpondern gespeichert werden. Die Daten, die jeweils nicht direkt auf den Transpondern abgelegt werden, sind in Datenbanken im Backend gespeichert und können von dort abgerufen werden.

Die zu einem Objekt verfügbaren Daten sind also immer die gleichen, nur sind sie mal auf den Transpondern und mal nur im Backend gespeichert. Es ist auch möglich, dass Daten sowohl direkt auf den Transpondern als auch im Backend gespeichert werden. Für die Betrachtungen im Rahmen dieses Dokuments ist jedoch nur interessant, welche Daten direkt auf den Transpondern verfügbar sind. Ob sie ausschließlich dort gespeichert sind oder auch redundant im Backend ist hier unerheblich, Redundanz für ausgewählte Daten kann aber in bestimmten Anwendungsfällen eine interessante Option darstellen.

Folgende Beispielszenarien sind dargestellt:

- ein Supermarktartikel (Abbildung 3),

	Identifizier und umfangreiche Daten	Mehrfach strukturierter Identifier	Minimal-Identifier mit Anwendungsbezug	Minimal-Identifier ohne Anwendungsbezug
ISBN	X			
Autor im Klartext	X			
Titel im Klartext	X			
Schlagworte im Klartext	X			
Bibliothek: Bibliothekskennung	X	X	X	X
Bibliothek: Mediennummer	X	X	X	X
Bibliothek: Ausleihstatus	X	X		
Bibliothek: Sicherung	X	X		
Anzahl Teile	X	X		
Verkaufspreis	X			
Klappentext	X			
Identifier der verwaltenden Stelle				X
Eindeutige Nummer innerhalb der verwaltenden Stelle				X

Abbildung 4: Praxisbeispiel: Buch aus Bücherei

	Identifizier und umfangreiche Daten	Mehrfach strukturierter Identifier	Minimal-Identifier mit Anwendungsbezug	Minimal-Identifier ohne Anwendungsbezug
Hersteller	X			
Pharmazentralnummer (PZN)	X	X	X	X
Chargennummer	X	X	X	
Seriennummer zum Eindeutigmachen	X	X	X	X
Mindesthaltbarkeitsdatum	X	X		
Verschreibungspflichtig	X	X		
Wirkstoff im Klartext	X			
Wirkstoffstärke	X			
Arzneiform (Darreichungsform)	X			
Packungsgröße	X			
Name im Klartext	X			
Beipackzettel	X			
Lagerungshinweise	X			
Identifier der verwaltenden Stelle				X
Eindeutige Nummer innerhalb der verwaltenden Stelle				X

Abbildung 5: Praxisbeispiel: Medikament

	Identifizier und umfangreiche Daten	Mehrfach strukturierter Identifier	Minimal-Identifier mit Anwendungsbezug	Minimal-Identifier ohne Anwendungsbezug
Verkehrsbetrieb	X	X	X	X
Fahrscheinart	X	X	X	
Fahrscheinnummer	X	X	X	X
Guthaben	X	X		
Ausstellungsdatum	X	X		
Gültigkeit	X	X		
Bisherige Fahrten	X			
Beförderungsbedingungen	X			
Identifier der verwaltenden Stelle				X
Eindeutige Nummer innerhalb der verwaltenden Stelle				X

Abbildung 6: Praxisbeispiel: Fahrschein eines Verkehrsbetriebs

- ein Buch aus einer Bücherei (Abbildung 4),
- ein Medikament (Abbildung 5),
- ein Fahrschein eines Verkehrsbetriebes (Abbildung 6).

2 Diskussion

Nach der im vorherigen Kapitel vorgenommenen Schilderung der Gestaltungsmöglichkeiten, inwieweit Daten direkt auf dem Transponder oder ausgelagert ins Backend gespeichert werden, werden nun die Auswirkungen der unterschiedlichen Möglichkeiten anhand praxisrelevanter Kriterien diskutiert.

2.1 Lesegeschwindigkeit und Fehlerrate

Für viele Anwendungen ist eine hohe Lesegeschwindigkeit von Bedeutung. Beispielsweise auf Fließbändern sollen pro Zeiteinheit möglichst viele Transponder erfassbar sein, um hohe Fördergeschwindigkeiten fahren zu können. Auch bei mobilen Lesegeräten ist eine schnelle Erfassung wichtig, insbesondere wenn viele Transponder im Pulk erfasst werden sollen. Benutzer wollen ungern auf die Beendigung eines Lesevorgangs warten.

Darüber hinaus ist es wichtig, dass Transponder nicht nur schnell sondern auch ohne Fehler erfasst werden. Nur so kann eine hohe Datenqualität gewährleistet werden und ein RFID-System einen produktiven Einsatz finden.

Sowohl für die Lesegeschwindigkeit als auch für die Fehlerrate ist die drahtlose Verbindung zwischen Transpondern und Lesegeräten der ausschlaggebende Faktor. Diese Verbindung hat

eine bestimmte Datenübertragungsrate und eine bestimmte Bitfehlerrate (bit error rate – BER). Diese Parameter sind abhängig vom eingesetzten Übertragungsstandard und den Umgebungseinflüssen. Beide Parameter haben von der zu übertragenden Datenmenge abhängige Auswirkungen: Bei gegebener Übertragungsrate dauert die Übertragung umso länger, je mehr Daten übertragen werden müssen. Der Zusammenhang ist linear. Bei fester Bitfehlerrate steigt die Wahrscheinlichkeit eines Übertragungsfehlers mit wachsender zu übertragender Datenmenge. Der Zusammenhang ist nichtlinear, mit wachsender Datenmenge geht die Wahrscheinlichkeit eines Fehlers asymptotisch gegen 100 %.

Die Folgerung ist, dass für eine hohe Lesegeschwindigkeit und eine geringe Fehlerrate die zu übertragende Datenmenge möglichst gering sein sollte. Das bedeutet, dass die notwendigsten Daten, d.h. nur Identifier, auf den Transpondern gespeichert werden sollten. Andere Daten sollten im Backend vorgehalten werden, wo hohe Netzwerkbandbreiten und verlässliche Übertragungskanäle vorhanden sind.

Werden Daten teilweise im Backend gespeichert, so müssen diese dort abgerufen werden, bevor sie am Ort des Lesens des Tags verfügbar sind. Dies stellt mit heutigen IT-Infrastrukturen unternehmensintern kaum mehr einen limitierenden Faktor dar. Werden Daten von anderen Unternehmen bereitgestellt, kann es sinnvoll sein, diese als sogenannte „vorlaufende Daten“ bereits vorab bereitzustellen. Das bedeutet z.B., dass wenn ein Objekt mit einem bestimmten Ziel ein Unternehmen verlässt, die Daten bereits während dem physikalischen Transport dem Zielunternehmen zur Verfügung gestellt werden.

Ergänzend anzumerken ist noch, dass bei einer Speicherung weiterer Daten auf den Transpondern das System zur Optimierung so gestaltet werden kann, dass nicht immer alle auf einem Transponder verfügbaren Daten abgerufen werden sondern nur die gerade benötigten. Der grundsätzliche Nachteil der Datenspeicherung auf den Transpondern bleibt jedoch bestehen.

2.2 Flexibilität

In Zeiten sich ändernder Anforderungen, denen sich Unternehmen umgehend anpassen müssen, ist Flexibilität von enormer Bedeutung. Die flexibelsten Lösungen hinsichtlich der Datenspeicherung in RFID-Systemen sind eindeutig die, bei denen ausschließlich Identifier auf den Transpondern und möglichst viele Daten im Backend gehalten werden. Dafür gibt es mehrere Gründe, die im Folgenden erläutert werden.

Ein Argument für die ausschließliche Speicherung von Identifiern auf Transpondern ist die Kompatibilität zu Barcodesystemen. Häufig ist es heute so, dass Barcodes eingesetzt werden und diese erst bei hochpreisigen Produkten, später zunehmend auch bei günstigeren, durch RFID-Transponder ergänzt werden. Dies liegt daran, dass Barcodes extrem kostengünstig sind, RFID jedoch eine bequemere Handhabung oder erhöhte Sicherheit gegen Produktfälschungen bietet. In derartigen gemischten Szenarien ist es möglich, die gleichen Daten sowohl auf einem Barcode (i.d.R. aus Platzgründen ein 2D-Barcode) und einem RFID-Transponder zu speichern. Barcode und Transponder fungieren dann bezüglich der Objektidentifikation als reine Datenträger, wobei es für die weiteren Prozesse gleichgültig ist, ob der Barcode oder der Transponder gelesen wird. Um die für den Barcode benötigte Fläche klein zu halten, sollte die zu speichernde Datenmenge minimal sein, sodass ausschließlich Identifier als Barcodes bzw. auf den Transpondern gespeichert werden sollten.

Barcodes bzw. Transponder mit weltweit eindeutigen Identifiern ermöglichen auch die Verwendung über Unternehmensgrenzen hinweg. Nicht jedes Unternehmen muss einen eigenen Datenträger aufbringen (und evtl. die anderer Unternehmen entfernen), sondern kann den bereits vorhandenen zur eindeutigen Identifikation des jeweiligen Objektes nutzen. Zusätzlich vorhandene Daten stören zwar grundsätzlich nicht, doch kann ein Unternehmen nicht einfach eine beliebige Menge weiterer Daten hinzufügen. Es müsste sichergestellt sein, dass die Transponder genügend Speicher haben und dieser nicht mit Zugriffsbeschränkungen behaftet ist. Insbesondere wenn ein Unternehmen mit vielen anderen in einer Lieferkette zusammenarbeitet, ist eine derartige Abstimmung schwierig vorzunehmen. Die Verknüpfung der Transponder-Identifizier mit beliebigen Daten im Backend ist jedoch stets ohne jegliche Abstimmung möglich, sodass unternehmensübergreifende RFID-Systeme so einfacher zu implementieren sind und die Kompatibilität zu Barcode-Systemen (auf denen keine Daten nachträglich ergänzt werden können) gewahrt bleibt.

Ein weiterer Vorteil der Datenhaltung im Backend statt auf den Transpondern ist, dass Daten ohne Anwesenheit der Transponder in der Reichweite eines Lesegerätes geändert werden können. Dies kann in bestimmten Situationen enorme Vorteile aufweisen – insbesondere wenn der Ort, an dem sich die Transponder befinden, außerhalb der administrativen Einflussnahme ist.

Mit diesem Vorteil verbunden ist auch die Aktualität der Daten. Im Backend kann immer die aktuelle Datenversion vorgehalten werden. So macht es etwa Sinn, dass der Beipackzettel eines Medikamentes nicht auf dem Transponder des Medikamentes sondern im Backend gespeichert wird, weil dann immer die aktuellste Version zurückgeliefert werden kann. Nur so kann sichergestellt werden, dass z.B. auch die neuesten Informationen über Nebenwirkungen o.ä. direkt verfügbar sind.

Eine Datenspeicherung im Backend ist auch flexibel hinsichtlich der Änderung von zu speichernden Daten. In Datenbanken im Backend können auf einfache Weise zusätzliche Datenfelder ergänzt oder nicht mehr benötigte gelöscht werden. Eine Anpassung hin zu den aktuellen Anforderungen ist damit vergleichsweise einfach möglich. Bei einer Datenspeicherung auf Transpondern hingegen wären, zumindest zeitweise, Transponder mit unterschiedlichen Datenbeständen im Umlauf, was zu längeren Übergangszeiten und höherer Komplexität führen würde.

2.3 Sicherheit

Die Datenübertragung zwischen Transpondern und Lesegeräten findet über die Luft als Übertragungsmedium statt. Dieses Medium ist öffentlich, sodass die übertragenen Daten leicht mitgehört werden können. Die Nutzung kryptographischer Protokolle zur Wahrung der Vertraulichkeit ist zwar grundsätzlich möglich, doch sind Transponder mit derart erweiterter Funktionalität von der Betrachtung in diesem Beitrag ausgeschlossen. Oftmals scheidet die Nutzung von Transpondern mit derartiger Funktionalität auch aus Kostengründen aus. Ein Transponder kann damit für die hier angestellten Betrachtungen als Datenträger betrachtet werden, auf dem zwar verschlüsselte Daten gespeichert werden können, der jedoch nicht in der Lage ist, selbsttätig kryptographische Operationen durchzuführen.

Werden unverschlüsselte Daten auf Transpondern gespeichert, kommt dies einer Veröffentlichung gleich, da die Daten beim Auslesen mitgehört werden können oder die Transponder

auch unbemerkt ausgelesen werden können. Nur so lange die Transponder in geschlossenen Bereichen bleiben, wie etwa in einer Werkshalle, kann diese Bedrohung vernachlässigt werden. Somit ist es sinnvoll, möglichst viele Daten im Backend zu speichern, weil sie dann nicht über einen ungesicherten Kanal übertragen werden müssen und der Zugriff feingranular geregelt werden kann. In den Unternehmensnetzwerken können Daten gesichert übertragen werden (SSL/TLS/o.ä.) und auch ein Zugriff auf die Daten flexibel kontrolliert werden, was bei auf Transpondern gespeicherten Daten so nicht möglich ist.

Die Speicherung verschlüsselter Daten auf Transpondern ist in Bereichen sinnvoll, bei denen eine zentrale Datenhaltung vermieden werden soll. Dies ist beispielsweise bei den deutschen Reisepässen bezüglich der biometrischen Daten derzeit der Fall.

Ein weiterer Sonderfall, bei dem das Speichern von Daten – am besten, aber nicht notwendigerweise – verschlüsselt zweckmäßig ist, ist gegeben, wenn es sich um Daten handelt, die einmal geschrieben werden und dann niemals mehr verändert werden dürfen, nicht einmal durch die den Transponder ausgebende Stelle selbst. Dies könnte z.B. bei zum Verbraucherschutz eingeführten regulatorischen Bestimmungen der Fall sein. Dass Daten nicht mehr geändert werden können, kann bei im Backend gespeicherten Daten nicht garantiert werden, da zumindest der Datenbankbetreiber die dort gespeicherten Daten noch verändern kann.

Die Speicherung von Daten auf den Transpondern ist hingegen zu vermeiden, wenn Daten öfter geändert werden müssen und eine unerlaubte Veränderung der gespeicherten Daten verhindert werden soll. Letztere könnte nur durch Zugriffskodes geschehen, die jedoch aufgrund der ungesicherten Datenübertragung zwischen Transpondern und Lesegeräten mitgehört werden können. Derartige Sicherheitsprobleme sind bei einer Datenspeicherung im Backend nicht gegeben, da hier die Rechenleistung und die Flexibilität gegeben ist, dass Authentifizierungs- und Verschlüsselungsverfahren nach dem jeweils aktuellen Stand der Technik eingesetzt werden können.

Für das Führen einer Produkthistorie im Rahmen des sogenannten „Track & Trace“-Ansatzes sind randomisierte Identifier zweckmäßig. Das bedeutet, dass der Seriennummernanteil des Identifiers nicht fortlaufend oder nach einem anderen festen Schema sondern zufällig vergeben wird. Hintergrund ist, dass auf diese Weise vergebene Identifier nicht erraten werden können, was einige Angriffsmöglichkeiten nimmt.

2.4 Datensicherheit und Schutz der Privatsphäre

Wie bereits im vorherigen Abschnitt beschrieben, können unverschlüsselt auf den Transpondern gespeicherte Daten während des Auslesens mitgehört werden oder durch Lesegeräte direkt abgefragt werden. Zur Vermeidung dieser Bedrohungen bietet es sich an, möglichst viele Daten im Backend zu speichern, wo Daten verschlüsselt übertragen werden können und eine effektive und flexible Zugriffskontrolle in kostengünstiger Weise implementierbar ist.

Verlassen Transponder mit gespeicherten Daten den Bereich des Werksgeländes einen Unternehmens, der als physikalisch geschützt erachtet werden kann, so ist aus Datenschutzgründen die Löschung aller nicht mehr benötigten Daten von den Transpondern zweckmäßig. Nur so können mögliche Bedrohungen durch Industriespionage vermieden werden und dem Grundsatz der Datensparsamkeit Rechnung getragen werden. Außerhalb des Werkes könnten die

Daten ausgelesen werden. Der Aufwand für die Löschung kann vermieden werden, indem möglichst wenige Daten direkt auf den Transpondern gespeichert werden.

Gesetzgebung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterliegt dem Bundesdatenschutzgesetz in vollem Umfang. Dies schließt grundsätzlich die Datenspeicherung auf Transpondern genauso wie die Speicherung im Backend ein. Aus den schon genannten Gründen ist jedoch eine Speicherung im Backend vorzuziehen, weil dort der Zugriff auf die Daten effektiv kontrollier- und protokollierbar ist.

Schwieriger einzuschätzen ist die rechtliche Situation bei nicht personenbezogenen Daten. Derartige Daten können, wenn Transponder in den Bereich von Verbrauchern gelangen, als „potenziell personenbeziehbar“ eingestuft werden [DB2008]. Diese Einstufung reicht erst einmal nicht aus, um das Bundesdatenschutzgesetz in Anwendung zu bringen, doch bewegen sich beteiligte Unternehmen, etwa bei zufälligem Auslesen von Daten auf Transpondern, schnell in eine Grauzone [DB2008]. Zur Vermeidung derartiger Probleme sollten möglichst wenige Daten direkt auf den Transpondern gespeichert werden, wenn die Transponder in den Bereich von Verbrauchern gelangen.

Auch aus anderen Gesetzen lässt sich die Zweckmäßigkeit derartiger Vorsorge zur Vermeidung rechtlicher Probleme ableiten: „Am 15.12.1983 sprach das Bundesverfassungsgericht das sogenannte Volkszählungsurteil. Im Rahmen dieses Urteils kritisierte das Gericht das überhand nehmende Informationsbegehren des Staates über seine Bürger und stellte das Recht auf informationelle Selbstbestimmung heraus, welches als weitere Ausprägung den allgemeinen Persönlichkeitsrechten hinzugefügt wurde. Die informationelle Selbstbestimmung entstand so durch richterliche Rechtsfortbildung aus den Artikeln 1 (1) GG (Menschenwürde) und 2 (2) GG (allgemeine Handlungsfreiheit) des Grundgesetzes. Das Urteil des BVerfG nahm den Gesetzgeber in die Pflicht und ist damit die Basis des deutschen Datenschutzrechts [...] Während die Artikel 1 und 2 des Grundgesetzes Abwehrrechte des Bürgers gegen den Staat darstellen, gehen die vom Bundesverfassungsgericht im Zuge richterlicher Rechtsfortbildung aus ihnen formulierten allgemeinen Persönlichkeitsrechte, zu denen auch die ISB [Informationelle Selbstbestimmung] gehört, darüber hinaus. Sie sind als allgemeines Rechtsgut auch im Zivilrecht i.S. des § 823 BGB etabliert.“ [Wac2006]

Akzeptanz durch Datensparsamkeit auf Transpondern

Unabhängig von den rechtlichen Erfordernissen ist auch zu berücksichtigen, dass die RFID-Technologie ihre Vorteile nur in allen Lebensbereichen entfalten kann, wenn die Bevölkerung die Technologie annimmt. In der Presse werden unterschiedlichste Szenarien geschildert, die mögliche Bedrohungen darstellen. Dies schließt Szenarien ein, die nicht einmal RFID-spezifisch sind (z.B. an der Supermarktkasse die Verknüpfung der gekauften Waren mit der Person über eine Kunden-/Kreditkarte – dies ist heute mit Barcodes auch schon ohne weiteres möglich) und damit die seriöse Diskussion um wirkliche Bedrohungen weiter erschweren. In jedem Fall sollte das Design von RFID-Systemen so ausgelegt sein, dass eine höchstmögliche Akzeptanz erzielt wird.

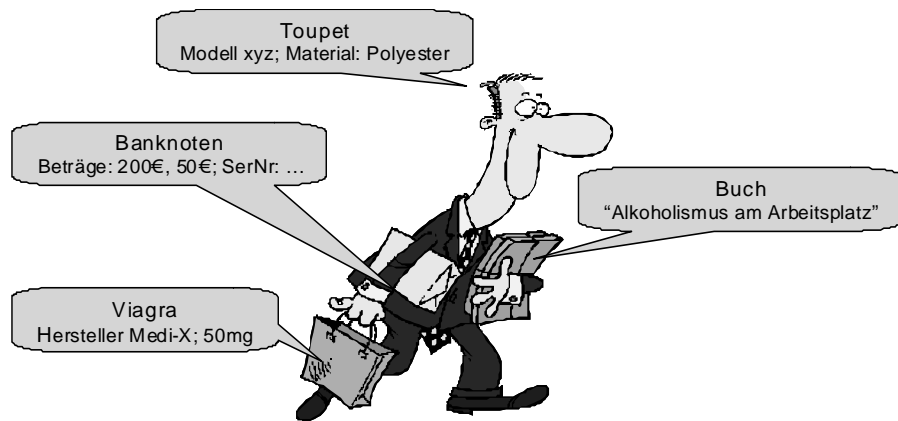


Abbildung 7: Beispiel für Privatsphäreproblem [Bild: Juels]

Daten auf Transpondern können mit Lesegeräten unbemerkt ausgelesen werden. Auch ein Mithören von Lesevorgängen ist möglich. Dabei muss davon ausgegangen werden, dass die üblicherweise erzielbaren Reichweiten (je nach genutzter Frequenz von wenigen Zentimetern bis hin zu wenigen Metern bei passiven Transpondern) mit geeigneter Technik um ein Vielfaches übertroffen werden können. So können Lesegeräte beispielweise unerlaubt hohe Feldstärken verwenden. Durch Nutzung technischer Kniffe können aus 10 cm Reichweite leicht 50 cm werden [KW2005]. Auch in anderen wissenschaftlichen Veröffentlichungen wird von hohen zu erreichenden Reichweiten berichtet (z.B. [SWE2003]), insbesondere was das Abhören von Lesevorgängen betrifft.

Die Auswirkungen der Datenspeicherung auf Transpondern hängen selbstverständlich von Art und Umfang der gespeicherten Daten ab. Um eine Diskussionsgrundlage zu haben, ist in Abbildung 7 ein Beispiel dargestellt.

Man stelle sich vor, man könnte im Vorbeigehen die in den Sprechblasen angegebenen Informationen zur in Abbildung 7 dargestellten Person auslesen. Wie man sieht, können vertrauliche Informationen, z.B. über den Gesundheitszustand darunter sein, oder Informationen, die man aus Scham vielleicht nicht preisgeben möchte. Werden RFID-Transponder auch zur Fälschungssicherung von Banknoten eingesetzt, so könnte ein Taschendieb vor der Tat prüfen, ob sich ein Diebstahl lohnt.

Das Privatsphäreproblem in diesem Beispiel kommt durch eine Zusammenführung von für sich genommen harmlosen Einzelinformationen zu Stande. Diese Einzelinformationen sind im Einzelnen:

- die Zuordnung zwischen Personen und Objekten
Man sieht, dass die Person Gegenstände mit sich führt, bzw. erkennt, dass die ausgelesenen RFID-Transponder zu Gegenständen gehören, die die Person mit sich führt.
- die Zuordnung zwischen Objekten und RFID-Transpondern
Transponder sind an Gegenständen angebracht.
- RFID-Transponder haben Informationen zugeordnet
Die auf den RFID-Transpondern gespeicherten Daten haben eine Bedeutung, bzw. mit den Transpondern sind ungesicherte Daten in Datenbanken assoziiert.

Alle Einzelinformationen sind relativ harmlos. So enthalten die RFID-Transponder beispielsweise keine persönlichen Daten. Wie das Beispiel zeigt, können sich die Einzelinformationen jedoch im Zusammenspiel zu einem detaillierten Bild zusammenfügen und damit die Privatsphäre durchaus bedrohen.

Um das Problem gänzlich zu vermeiden, dürften die auf den RFID-Transpondern gespeicherten Daten keine direkte Bedeutung haben. Somit ist aus Sicht des Schutzes der Privatsphäre zu raten, so wenige Daten wie möglich direkt auf Transpondern zu speichern und den Daten, die dort gespeichert werden müssen, jegliche interpretierbare Bedeutung zu nehmen.

Selbst die Angabe von Hersteller, Produktschlüssel und Seriennummer ist bereits zu viel, wie das Beispiel aufzeigt. Dennoch ist zurzeit im Handel geplant, alle Produkte mit einem RFID-Transponder auszustatten, der mindestens Hersteller, Produkttyp und Seriennummer in Form eines mehrfach strukturierten Identifiers enthält. Ursache ist, dass die Entwickler des Standards von gewohnten Barcode-Systemen ausgegangen sind und diese einfach angepasst und erweitert haben, statt sie auf die Eigenarten der RFID-Technologie zuzuschneiden.

Zuweilen wird argumentiert, dass es sich bei diesen Identifiern um reine Zahlen handele, aus der sich keine Klartextbedeutung erschließen lasse. Die Zuordnungen zwischen den Kennungen, die für die jeweiligen Hersteller und Produkttypen bestehen, und den Herstellern und Produkttypen „im Klartext“ müssen erst einmal bekannt sein, bevor ein Privatsphäreproblem entstehen könne.

Dieses Argument kann man in keiner Form gelten lassen. Zum einen ist die Zuordnung zwischen Kennungen und Herstellern/Produkttypen jedem Warenwirtschaftssystem bekannt, so dass sie nicht geheim gehalten werden kann, zum anderen lassen sich leicht Tabellen mit der Zuordnung von Hand erstellen. Für das bekannte EAN-System ist sogar eine offizielle Datenbank frei verfügbar [GEPIR]. Daneben gibt es eine Reihe Community-betriebener Datenbanken im In- und Ausland, etwa [EAN1], [EAN2] und [EAN3]. Es ist davon auszugehen, dass auch für den EPC (Electronic Product Code) derartige Datenbanken vorhanden sein werden, auf die jedermann Zugriff hat.

Aus Privatsphäregründen sollten RFID-Transponder somit nur minimal strukturierte Daten enthalten, d.h. eine verwaltende Stelle und eine innerhalb dieser Stelle eindeutige Seriennummer. Im Idealfall ist die verwaltende Stelle so gewählt, dass kein Bezug zum Objekt, das mit dem Transponder ausgestattet ist, gegeben ist. Die verwaltende Stelle sollte also im Idealfall weder der Hersteller, noch der Besitzer oder Eigentümer des Objektes sein, da bereits eine derartige Angabe entscheidende Hinweise auf die Beschaffenheit des Produktes, z.B. die Wertigkeit, geben kann.

Im vorherigen Unterkapitel 2.3 wurde ein Sonderfall betrachtet, in dem Daten auf Transpondern gespeichert werden sollten, wenn die Daten unabänderlich sein oder nicht zentral gespeichert werden sollen. Um keine Informationen über das jeweilige Objekt preiszugeben, sollten diese Daten verschlüsselt auf den Transpondern gespeichert werden. Der erforderliche Schlüssel zum Entschlüsseln kann dann im Backend mit einem Zugriffsschutz versehen abgelegt werden. Alternativ kann der Schlüssel auf das Objekt aufgedruckt sein, wie es beispielsweise für das Passbild im Reisepass gehandhabt wird.

Location Privacy

Ein anderes Privatsphäreproblem ergibt sich, wenn eine Person Objekte mit RFID-Transpondern ständig mit sich führt. Beispiele sind Armbanduhren, Brillen oder Schuhe. Dann ist die sogenannte „Location Privacy“ bedroht: Dadurch, dass von einem Lesegerät öfter der gleiche Transponder registriert wird, kann darauf geschlossen werden, dass es sich höchstwahrscheinlich um die gleiche Person handelt. Diese Information kann zur Erstellung von Bewegungsprofilen oder zum Erfassen von Konsumgewohnheiten verwendet werden.

Ein verwandtes Problem würde auftreten, wenn Reifenhersteller Reifen mit Transpondern ausstatten würden. Tankstellenketten könnten mittels installierter Lesegeräte unbemerkt Profile erstellen, wer, wo, wie oft tankt, und durch Vernetzung einzelner Tankstellen auch die grobe Reiseroute oder Lebensgewohnheiten ihrer Kunden rekonstruieren.

Dies sind keine fiktiven Szenarien: Ein Reifenhersteller hat vor einigen Jahren bekannt gegeben, seine Produkte mit RFID-Transpondern ausstatten zu wollen. Verbraucherproteste haben daraufhin zu einem negativen Image geführt, sodass von diesem Plan wieder Abstand genommen wurde.

Die Erstellung derartiger Bewegungsprofile ist mit Transpondern möglich, auf denen beliebige statische Daten gespeichert sind, die die notwendige Eindeutigkeit haben. Hier ist ein eindeutiger Identifier ausreichend. Auch verschlüsselte Daten können missbraucht werden. Dadurch, dass es sich immer um die gleichen Daten handelt, kann geschlossen werden, dass es sich um den gleichen Transponder und damit das gleiche Objekt handelt.

Eine Lösung böte hier nur die Speicherung unstrukturierter Identifier, die sich regelmäßig ändern, sodass Außenstehende nicht erfassen können, dass es sich ggf. um das gleiche Objekt handelt. Dazu sind Transponder mit zusätzlicher Funktionalität erforderlich, sodass diese Möglichkeit im Rahmen dieses Beitrags nicht weiter betrachtet wird.

2.5 Kosten

Die Kosten für ein RFID-System sind ein ganz wesentlicher Punkt, wenn es zur Produktivitäts- und Effizienzsteigerung von Prozessen eingesetzt werden soll. Zu betrachten sind die Kosten für die Transponder als auch für die Infrastruktur bestehend aus Lesegeräten und den Backend-Systemen.

In den vorangegangenen Abschnitten sind einige Faktoren, die indirekt Kosten bewirken, bereits betrachtet worden. So wirken sich beispielsweise Zeitverluste durch zu geringe Lesegeschwindigkeiten auch monetär aus. In diesem Abschnitt wird im Folgenden auf die direkten Kosten eingegangen.

Transponder werden in hohen Stückzahlen benötigt, um alle zu identifizierenden Objekte damit ausstatten zu können. Dies ist insbesondere in Anwendungsszenarien der Fall, in denen Transponder nicht wiederverwendet werden können. Der wesentliche Kostenfaktor für viele Anwendungsszenarien ist somit der Stückpreis der RFID-Transponder.

Der Stückpreis der Transponder hingegen ist abhängig von deren Fähigkeiten, d.h. unter anderem der Menge des verfügbaren Speichers und evtl. bereit gestellter Zusatzfunktionalität. Je größer die Fähigkeiten, desto teurer der Transponder. Ein wesentlicher Punkt ist darüber hinaus die Stückzahl der Transponder im Herstellungsprozess. Ein Transpondertyp kann in

Millionenstückzahlen günstiger produziert werden als in Stückzahlen, die eine oder mehrere Größenordnungen darunter liegen.

In Konsequenz sollten möglichst viele Anwendungen den gleichen Typ von Transpondern einsetzen, die darüber hinaus auch noch eine möglichst geringe Funktionalität haben sollten. Der gemeinsame Nenner sind Transponder, die ausschließlich einen weltweit eindeutigen Identifier speichern können. Über die Struktur dieses Identifiers, d.h. in welche Teile er aufgeteilt wird, kann aus Sicht der Transponderkosten nichts ausgesagt werden. Die Aufteilung ist aus Kostensicht beliebig.

Bezüglich der Infrastrukturkosten werden in jedem Fall Lesegeräte benötigt. Diese sind immer notwendig, gleichgültig ob Daten nun direkt auf Transpondern oder im Backend gespeichert werden.

Unterschiede können sich prinzipiell jedoch bei den Kosten für die IT-Infrastruktur, d.h. Kosten für Installation, Wartung und Betrieb des Backends und der Kommunikationsinfrastruktur ergeben. Sind alle Daten direkt auf den Transpondern gespeichert, können sie direkt auch von mobilen Lesegeräten erfasst werden. Eine Kommunikation mit Backendsystemen ist dafür erst einmal nicht erforderlich, sodass auch keine entsprechende Infrastruktur benötigt wird. Da eine derartige Infrastruktur im Regelfall eine hohe Verfügbarkeit haben muss, kann es sich hierbei um nicht unerhebliche Kosten handeln.

In der Praxis ist es allerdings bei den meisten Anwendungsfällen so, dass eine derartige Infrastruktur ohnehin benötigt wird. Beispielsweise soll oft ein Abgleich mit Daten im Warenwirtschaftssystem erfolgen. In derartigen Fällen, die eher die Regel als die Ausnahme darstellen, ergeben sich also keine zusätzlichen Kosten für Errichtung und Betrieb der Infrastruktur. Von Seiten der Infrastrukturkosten her ist es dann nahezu unerheblich, ob Daten direkt auf Transpondern oder im Backend gespeichert werden. Je nach Anwendung gibt es Tendenzen in einzelne Richtungen, die jedoch letztendlich kaum ins Gewicht fallen.

3 Einschätzung und Empfehlung

Es kann davon ausgegangen werden, dass mit zunehmender Reife und mit fallenden Preisen für die RFID-Technik der Einsatz über die Jahre zunehmen wird, d.h. RFID auch in Bereichen eingesetzt werden kann, wo die Technik zuvor noch zu unzuverlässig oder zu teuer war.

Für Unternehmen und Dienstleister stellt sich in jedem Fall die Frage der technischen Ausgestaltung der RFID-Systeme. Eine der zu klärenden Fragen ist, welche Daten direkt auf Transpondern und welche in Backend-Systemen gespeichert werden sollten. Dieser Frage wurde im Rahmen dieses Beitrags nachgegangen. Dazu wurden zuerst die Möglichkeiten erklärt und an Beispielen klar gemacht, bevor dann die Auswirkungen diskutiert wurden.

In Tabelle 8 ist zusammenfassend dargestellt, welche Auswirkungen die Wahl der technischen Ausgestaltung hinsichtlich der einzelnen betrachteten Kriterien hat. Fett gedruckte Kreuze bezeichnen eine aus Sicht der Erfüllung des Kriteriums optimale Lösung. Normal bzw. in Klammern gedruckte Kreuze bezeichnen Fälle, in denen das Kriterium mehr oder weniger berücksichtigt wird. Die Tabelle berücksichtigt keine Sonderfälle, sondern gibt nur die generelle Tendenz wieder.

	Identifizier und umfangreiche Daten	Mehrfach strukturierter Identifier	Minimal-Identifier mit Anwendungsbezug	strukturloser Minimal-Identifier	wechselnder Identifier	
Lesegeschwindigkeit und Fehlerrate		X	X	X	X	X
Flexibilität		(X)	X	X	X	X
Sicherheit			(X)	X	X	X
Datenschutz / Schutz der Privatsphäre				(X)	X	X
Kosten		(X)	X	X	X	(X)

Abbildung 8: Zusammenfassung der Auswirkungen

Betrachtet man die Tabelle, so sieht man, dass die für den Schutz der Privatsphäre optimale Lösung diejenige mit wechselnden Identifiern darstellt. Aufgrund der höheren Kosten dieser Lösung im Vergleich zu anderen sowie anderer Einschränkungen ist diese Variante nur sinnvoll, wenn sie gesetzlich vorgeschrieben ist und überall Anwendung findet. Eine derartige gesetzliche Regelung ist jedoch weder in Kürze noch längerfristig zu erwarten.

Alle Kriterien zusammengenommen ist die Lösung, nur einen Minimal-Identifier ohne Anwendungsbezug direkt auf den Transpondern und alle anderen Daten im Backend zu speichern, die sinnvollste. Diese Variante ermöglicht hohe Lesegeschwindigkeiten, sodass in kurzer Zeit auch eine große Anzahl von Transpondern im Pulk erfasst werden kann. Durch die Flexibilität der Datenspeicherung im Backend sind unterschiedlichste Anwendungen und auch Änderungen an bestehenden Anwendungen vergleichsweise leicht durchzuführen. Es werden auch keine verwertbaren Daten über die Luft übertragen, die abgehört werden könnten, oder Daten auf Transpondern gespeichert, die ausgelesen und missbraucht werden könnten. Eine effektive Zugriffskontrolle, Verschlüsselung usw. ist im Backend vergleichsweise einfach, flexibel und kostengünstig zu bewerkstelligen. Damit ist die Privatsphäre (von Personen, aber auch von Unternehmen) besser zu schützen als bei Speicherung von Daten in Transpondern, die nicht aus technischer Notwendigkeit heraus dort vorgehalten werden müssen. Dies führt auch zu einer hohen Investitionssicherheit in Bezug auf möglicherweise erfolgende regulatorische Anforderungen. Weitergehende Schutzmaßnahmen, die ungewollte Wiedererkennung von Objekten und Personen und damit das Erstellen von Bewegungsprofilen effektiv zu verhindern vermögen, bleiben hier außen vor, da der damit verbundene Aufwand hoch ist. Die Lösung, nur Minimal-Identifier ohne Anwendungsbezug auf Transpondern zu speichern, ist aus Kostensicht eine sehr erstrebenswerte.

Entscheidern und Entwicklern kann damit die Empfehlung gegeben werden, RFID-Systeme dergestalt zu fordern und zu entwickeln, dass nur eine minimale Datenmenge direkt auf Transpondern gespeichert wird, d.h. ein Minimal-Identifier, der aus Datenschutzgründen keinen Anwendungsbezug haben sollte. Alle anderen Daten können flexibel in Backendsystemen vorgehalten werden.

Literatur

- [Hen2008] Dirk Henrici: *RFID Security and Privacy – Concepts, Protocols, and Architectures*, Springer-Verlag, Heidelberg, 2008.
- [DB2008] Deutscher Bundestag: *Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie*, Unterrichtung durch die Bundesregierung, 2008.
- [Wac2006] Winfried Wacker: *informationelle Selbstbestimmung*, <http://www.realname-diskussion.info/isb.htm>, 2006.
- [KW2005] Ziv Kfir und Avishai Wool: *Picking virtual pockets using relay attacks on contactless smartcard systems*, IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm, 2005.
- [SWE2003] Sanjay E. Sarma, Stephen A. Weis und Daniel W. Engels: *Radio-Frequency Identification: Security Risks and Challenges*, Cryptobytes, RSA Laboratories Vol. 6, Nr. 1, S. 2–9, 2003.
- [GEPiR] *GEPiR - Die gelben Seiten von GSI*, http://www.gepir.de/v31_client/
- [EAN1] *Open EAN/GTIN Database*, <http://openean.kaufkauf.net/>
- [EAN2] *EAN-Suche*, <http://www.ean-suche.de/>
- [EAN3] *Codecheck*, <http://www.codecheck.ch/>