DuD
Datenschutz und Datensicherheit

RFID und Datenschutzrecht

Risiken, Schutzbedarf und Gestaltungsideen

Jürgen Müller, Matthias Handy

Der vorliegende Artikel gibt einen Überblick über rechtliche Risiken beim Einsatz von RFID-Systemen und leitet daraus einen entsprechenden Schutzbedarf ab. Zur Sicherung der datenschutzrechtlichen Zweckbindung werden unter anderem eine Anwendungskennung (AK) und eine Verwendungskennung (VK) vorgeschlagen, die bestimmte Verarbeitungsbeschränkungen von Daten gegenüber verantwortlichen Stellen deutlich machen.[1]

Ass. jur.
Jürgen Müller

Mitarbeiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel

E-Mail: j.mueller@uni-kassel.de

Dipl. Wirtsch.-Ing.
Matthias Handy

Mitarbeiter am Institut für Angewandte Mikroelektronik und Datentechnik an der Universität Rostock

E-Mail: matthias.handy@uni-rostock.de

[1] Der Beitrag entstand im Rahmen des von der Daimler-Benz-Stiftung geförderten Kollegs „Living in a Smart Environment“, http://www.smart-environment.de.

1 Einleitung

Die Einsatzmöglichkeiten von RFID-Systemen (Radio Frequency Identification) werden von Verbraucher- und Datenschützern weltweit kritisch diskutiert. Insbesondere in der angekündigten Einführung von RFID-basierten, elektronischen Produktkennzeichnungen (EPC) zum Ersatz des bisherigen Strichcodes im Einzelhandel, sieht man einen Angriff auf Anonymität und Privatsphäre des Kunden. Dagegen verspricht sich die Industrie durch den Einsatz von RFID-Systemen erhebliche Effizienzsteigerungen zum Beispiel durch kontaktlose Produkterfassung und Verfolgung von Waren sowie durch produktbezogene Kundeninformationssysteme.

2 Risiken von RFID-Systemen

2.1 Grundlegendes

Ein RFID-System besteht in seiner einfachsten Form aus einem Lesegerät und aktiven bzw. passiven Transpondern (RFID-Marken).[2] RFID-Lesegeräte setzen sich aus einer Steuerungseinheit und einer Hochfrequenzeinheit zusammen. Die Steuerungseinheit koordiniert und überwacht den Kommunikationsablauf mit dem Transponder, die Hochfrequenzeinheit erzeugt eine Trägerfrequenz und übernimmt die Aufgabe der Modulation bzw. Demodulation.

Eine passive RFID-Marke besteht üblicherweise aus einem Mikrochip (RFID-Chip) und einem Koppelelement (z.B. Antennenspule und Kondensator). Die erforderliche Energie wird bei induktiv gekoppelten passiven RFID-Marken dem magnetischen Wechselfeld des Lesegerätes entzogen.

[2] S. z. B. *Finkenzeller*, RFID-Handbuch, 2002.

Weltweit federführend bei der Entwicklung von RFID-basierter Produktkennzeichnung ist EPCglobal, ein Gemeinschaftsunternehmen der europäischen EAN international und des US-amerikanischen Uniform Code Council (UCC).[3] EPCglobal soll einen weltweiten Standard zur Produktkennzeichnung mittels RFID-Technologie entwickeln. Kern dieser Produktkennzeichnung ist der Elektronische Produkt-Code (EPC), eine weltweit eindeutige Nummer, die einem Produkt zugewiesen wird und anhand derer es entlang der Versorgungskette identifizierbar ist. Der EPC ist auf einem RFID-Chip gespeichert und kann von kompatiblen Lesegeräten ausgelesen werden. Der EPC ist eingebettet in das so genannte EPCglobal Network, einer Sammelbezeichnung für verschiedene Technologien, die mit der elektronischen Produktkennzeichnung verbunden sind: Der Object Name Service (ONS) gibt Auskunft darüber, wo Informationen zu dem entsprechenden Produktcode zu finden sind. Die Physical Markup Language (PML) ist eine standardisierte Form zur Beschreibung von Produktinformationen. Das Softwaresystem Savant verwaltet und transportiert sämtliche Informationen des Systems.

2.2 Technisch bedingte Einsatzmöglichkeiten

Danach lassen sich für RFID-Systeme vornehmlich als technische Bedingungen festhalten, dass sie in extrem kleinen Baugrößen mit einer Funkschnittstelle auf verschiedenen flexiblen Trägermaterialien aufgebracht werden können. Hieraus ergibt sich die Möglichkeit, RFID-Marken nicht nur sichtkontaktlos auszulesen, sondern auch mit Gegenständen unlösbar zu verbinden, unsichtbar zu platzieren und fast an und in jeden Gegenstand einzubringen. Da

[3] S. http://www.epcglobalinc.org

alle RFID-Marken in der Reichweite des Lesegerätfeldes erfasst werden, erfolgt das Auslesen und Beschreiben verhältnismäßig einfach, schnell und nahezu gleichzeitig.

RFID-Technik zeichnet sich daneben dadurch aus, dass die RFID-Marken mit einer weltweit eindeutigen Kennung und optional mit einem zusätzlichen Speicher für sonstige Daten ausgestattet sind sowie in ein Hintergrundsystem (z. B. ONS) mit weiterführenden Daten eingebunden werden können. Dies bedeutet die Identifizierbarkeit der RFID-Marke mit einer Art mehr oder weniger aussagekräftigen inhaltlichen Identität, je nach Umfang und Güte der auf der Marke selbst oder im ergänzenden Hintergrundsystem nachgewiesenen Daten.

Allerdings fehlt es bei RFID-Marken neben dem Lesegerät an einem direkten Ein- und Ausgabemedium, was keine Erkennbarkeit der datenverarbeitenden Vorgänge zum aktuellen Zeitpunkt erlaubt. Ebenso findet auf derzeitigen Marken keine Zugangs[4]- und Zugriffskontrolle[5] oder wenigstens eine Zugriffsprotokollierung statt. Dies bedeutet, dass die auf einer RFID-Marke abgelegten Daten hinsichtlich Auslesbarkeit und Manipulation offen zugänglich sind und keine Kontrolle über die Daten präventiv oder nachträglich ermöglichen.

Gleiches gilt für die Übertragung oder Kommunikation mit dem Lesegerät, die ebenfalls ungeschützt auf Grund fehlender Speicher- und Rechenkapazität auf den RFID-Marken ohne kryptographische Sicherungen abgewickelt wird. Diese Funkkommunikation ist aber in ihrer Reichweite sehr begrenzt, wodurch im Kreis der Reichweite eine gewisse Überschaubarkeit gewahrt bleibt.[6]

Prinzipiell lässt sich ein RFID-System mit herkömmlichen kryptographischen Verfahren gegen Angriffe sichern. Die besonderen Eigenschaften solcher Systeme erschweren jedoch die direkte Anwendung von Verfahren, wie sie beispielsweise bei Smart Cards zum Einsatz kommen. Dies ist zum Einen bedingt durch den drahtlosen Kommunikationskanal eines RFID-Systems, der Abhörangriffe erleichtert. Überdies sind kryptographische Verfahren auf (für RFID-Systeme) verhältnismäßig viel Speicher angewiesen. Auch die Energieversorgung und die Taktfrequenz sind oft nicht ausreichend, um aufwändige Verschlüsselungsverfahren durchzuführen. Schließlich erhöht die Integration kryptographischer Verfahren in RFID-Systeme den Preis solcher Systeme, vor allem den nach ökonomischen Gesichtspunkten kritischen Preis je RFID-Marke. Für einen weiträumigen Einsatz von RFID-Systemen beispielsweise im Einzelhandel ist jedoch ein hinreichend niedriger Stückpreis Voraussetzung.

[4] Authentifizierung des Lesegerätes.

[5] Verwaltung von Lese- und Schreibrechten.

[6] Reichweite von RFID-Systemen: eng gekoppelt (bis 1 cm), fern gekoppelt (bis 1 m) und long-range-Systeme (bis 10 m).

2.3 Konsequenzen der technischen Möglichkeiten

Die Möglichkeit der sichtkontaktlosen Kommunikation führt zur Unmerklichkeit der RFID-Kommunikation und zu einer gewissen räumlichen Distanz von der RFID-Marke zum Verwender derselben. Daher vermag der RFID-Marken-Inhaber auf Markenzugriffe nicht zu reagieren oder einzuschreiten. Ihm fehlt auch das Wissen, ob und auf welche Weise in einem bestimmten, zurückliegenden Zeitraum Zugriffe auf die RFID-Marke erfolgten.

Durch die Verbindung der RFID-Marken mit Gegenständen entstehen Kontextdaten, die zwangsläufig einen Gegenstandsbezug aufweisen. Wegen der Unlösbarkeit der RFID-Marke vom Gegenstand wird diese in das mit dem betreffenden Gegenstand verbundene Handeln der Menschen integriert. Eine Kontrolle der RFID-Technik ist so nur noch über den Nicht-Gebrauch des Gegenstandes möglich. Dagegen liegt in der Möglichkeit der schnellen, einfachen und quasi gleichzeitigen Erfassung die Voraussetzung eines allgegenwärtigen Einsatzes.

Die wichtigste Eigenschaft der RFID-Technik ist, dass die RFID-Marken durch das RFID-System wiedererkannt, Gegenständen und Personen zugeordnet, zu anderen, ebenfalls markierten Gegenständen in Beziehung gesetzt und aus einer Zusammenschau Muster erkannt werden können. Über Hintergrundsysteme lassen sich weiter führende Daten über die RFID-Marke und damit über den markierten Gegenstand, gleich einem Gedächtnis, abfragen. Dadurch können zusätzlich Datenspuren, insbesondere Bewegungsprofile der einzelnen RFID-Marke entstehen.

Da die Daten auf der RFID-Marke und die Funkkommunikation zum Lesegerät ungeschützt zugänglich sind, lässt sich ein unbefugtes Auslesen und Abhören der gespeicherten bzw. übermittelten Daten nicht verhindern. Diese unbefugte Zugriffsmöglichkeit birgt zudem ohne gesetzten Sperrbefehl (lock-command) die Gefahr der Manipulation der auf der Marke gespeicherten Daten.

Schließlich führen die fehlende Transparenz und Beeinflussbarkeit der datenverarbeitenden Vorgänge zu Kontrollverlust über die RFID-Technik durch den Betroffenen.

2.4 Verletzungspotenziale von Rechtsgütern

Die RFID-Technik ist eine Informations- und Kommunikationstechnik, die auf der einen Seite wegen ihrer Funkschnittstelle und der digitalen Inhalte im virtuellen Sozialraum angesiedelt ist und auf der anderen Seite durch die Verknüpfung zu einem körperlichen Gegenstand im realen Sozialraum präsent ist. Dadurch werden beim Einsatz von RFID-Systemen Interessen des Betroffenen berührt, die ihren Anker vornehmlich im Schutz des Eigentumsrechts (Art. 14 GG), der Handlungsfreiheit (Art. 2 Abs. 1 GG), der informationellen Selbstbestimmung (Art. 1 Abs. 1, 2 Abs. 1 GG) sowie des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) finden. Geltung kommt den Grundrechten auch gegenüber Privaten nicht nur über die grundrechtliche Ausstrahlungswirkung ins einfachgesetzliche Recht zu, sondern ihr objektiver Gehalt findet seinen Niederschlag in Vorschriften der übrigen Rechtsordnung. Bei RFID-Anwendungen sind die Grundrechte des Fernmeldegeheimnisses und der informationellen Selbstbestimmung besonders relevant.

Fernmeldegeheimnis

Das Fernmeldegeheimnis gemäß Art. 10 GG erfasst den Schutz von Kommunikationsbeziehungen. Daher wird durch § 89 TKG (2004) das unbefugte Kommunizieren über eine Luftschnittstelle, insbesondere das Auslesen und Beschreiben einer RFID-Marke bzw. ihrer Daten auch ohne Personenbezug strafbewehrt verboten, weil dies ein mit Abhören vergleichbarer Eingriff ist, obwohl der Vorgang vom Lesegerät initiiert und gesteuert wird.[7]

Im praktischen Umgang besteht die Schwierigkeit für den Verwender einer RFID-Marke, die subjektive Bestimmung

[7] Näher hierzu *Müller* DuD, 2004, 215 ff., aber noch zu § 86 TKG (1996). Auch nach § 89 TKG (2004) wird RFID-Kommunikation durch den Schutz des Abhörverbots erfasst. Wegen der Wortlautänderung des § 89 Satz 1 TKG (2004) könnte allerdings die Anwendung des § 89 TKG (2004) problematisch werden, wenn der Betreiber der Funkanlage und der Empfänger, für den die Nachricht bestimmt ist, auseinanderfallen.

der abgefragten und/oder empfangenen Daten durch den Markeninhaber, also das Befugtsein des RFID-Marken-Verwenders erkennen zu können.[8]

Informationelle Selbstbestimmung
Der Einsatz der RFID-Technik ist dann datenschutzrechtlich relevant, wenn auf dem RFID-Speicher selbst personenbezogene Daten abgelegt werden oder wenn die RFID-Marke mit ihrer Kennung (UID) oder den sonstigen abgespeicherten Daten (ggf. über den sie tragenden Gegenstand) einer Person zugeordnet werden kann. Dabei ist nicht nur das von keinem Zulassungstatbestand gedeckte Erheben, Verarbeiten oder Nutzen von Daten problematisch. Vielmehr entsteht bei den meist mobilen RFID-Anwendungen durch die Möglichkeit, Bewegungs- und Beziehungsmuster zu bilden, das Risiko, dass Profile aller Art generiert werden können.

3 Schutzbedarf

Durch den Einsatz von RFID-Systemen entstehen qualitativ neue Risiken. Zur Gewährleistung des Fernmeldegeheimnisses und der informationellen Selbstbestimmung bedarf es der Umsetzung von Schutzanforderungen, welche nach den Prinzipien des Datenschutzrechts gegliedert sind.

3.1 Eigentum und Besitz

Die Rechte aus einer Eigentums- oder Besitzposition erlauben grundsätzlich das Entfernen oder Deaktivieren einer an einem Gegenstand angebrachten RFID-Marke. Fremdbesitz (e contrario § 872 BGB), wenn zum Beispiel ein Kunde ein RFID-markiertes Fahrrad mietet, rechtfertigt kein Deaktivieren, da hier das bloße Vorhandensein einer RFID-Marke keine Besitzstörung nach § 858 Abs. 1 BGB darstellt.

3.2 Datensparsamkeit

Dem sich aus § 3a BDSG ergebenden präventiven Gestaltungsgebot der Datensparsamkeit lässt sich die Forderung entnehmen, RFID-Marken als potentiellen Gegenstand einer Datenverarbeitung zu deaktivieren oder zu entfernen.

3.3 Technisch-organisatorischer Schutz

§ 9a BDSG verlangt, die RFID-Kommunikation gegen Kenntnisnahme durch Dritte und die personenbezogenen Daten auf ihnen vor unbefugtem Zugang und Manipulation zu sichern.

3.4 Transparenz

Um dem Betroffenen die Verwirklichung seiner informationellen Selbstbestimmung zu ermöglichen, bedarf es der Transparenz datenverarbeitender Vorgänge. Daher muss zum Einen hinsichtlich des Einsatzes von RFID-Systemen ein Wissen um Art, Umfang und Struktur der datenverarbeitenden Vorgänge, insbesondere die Weise der Einbindung in ein Hintergrundinformationssystem (z. B. ONS) sichergestellt werden. Zum Anderen muss die Verwendung der personenbezogenen Daten sowie ihre Art und ihr Inhalt von der verantwortlichen Stelle dargelegt werden. Daneben gilt es, die erfolgenden datenverarbeitenden Vorgänge auf der RFID-Marke sowie zwischen Marke und Lesegerät erkennbar zu machen.

3.5 Zweckbindung

Die datenschutzrechtliche Zweckbindung soll sicherstellen, dass der Einzelne darauf vertrauen kann, dass die Datenverarbeitung nur zu dem von ihm oder dem Gesetz erlaubten Zweck erfolgt. Ein besonderes Risiko entsteht, wenn die personenbezogenen Daten über die Erhebung von der RFID-Marke hinaus gespeichert und genutzt werden. Daher muss, wenn schon technisch das Auslesen einer RFID-Marke nur schwer markenseitig gesteuert werden kann, zumindest die Weiterverarbeitung und zweckwidrige Verwertung ausgeschlossen werden.

Ein Problem grundsätzlicherer Natur ist das Erfordernis, die Zweckbindung und die Adressatenbestimmung der personenbezogenen Daten erkennbar zu machen.

3.6 Informationelle Gewaltenteilung

Die informationelle Gewaltenteilung fordert, bereichsspezifisch unterschiedliche Datenflüsse und -bestände gemäß dem Zweckbindungsprinzip streng getrennt zu halten. Einige Spezifikationen von RFID-Marken sehen in der Kennung neben der Seriennummer auch Daten inhaltlicher Natur vor.[9] Bei der ersten Anfrage des Lesegeräts (mit dem „Inventory-Befehl“) wird aber die Kennung in Gänze ausgelesen. Nachdem Daten in der Kennung, wie beispielsweise Produktklasse oder Produktkennziffer, ein anderer Zweck innewohnt als einer RFID-Seriennummer, gebietet der Gedanke der informationellen Gewaltenteilung und der des § 3a BDSG, innerhalb der RFID-Kennung Daten mit Seriennummernfunktion und Daten mit inhaltlicher Bestimmung zu trennen.

4 Gestaltungsvorschläge

4.1 Registrierbarkeit von Zugriffen auf RFID-Marken

Ein einfacher Ansatz zum Schutz vor unbemerktem Auslesen wäre ein Gerät, das die Aktivität von Lesegeräten erkennt und diese dem Nutzer anzeigt.[10] Zusätzlich könnte ein derartiger *Lesegerät-Warner* mit einer Protokollierungsfunktion ausgestattet werden, mit der sämtliche Lese- und Schreibvorgänge sowie -versuche aufgezeichnet werden können. Sinnvoll einsetzbar wäre der Warner allerdings nur, wenn auch jedes Lesegerät eindeutig identifizierbar ist.[11]

Auch auf der RFID-Marke können Zugriffe protokolliert werden. Vorstellbar wäre ein *Zugriffszähler*, der wie bei Webseiten die Zahl der Zugriffe mitzählt. Dafür könnte auf der Marke ein beispielsweise 8-bit großer Speicherbereich reserviert werden. Ein Zugriffszähler dieser Größe könnte bis zu $2^8 = 256$ Auslesevorgänge registrieren. Auf den ersten Blick erscheint diese Zahl zu gering, interessant ist bei einem derartigen Zähler jedoch nicht die absolute Zahl der Zugriffe, sondern lediglich die Anzahl der Zugriffe über einen bestimmten Zeitraum, beispielsweise während eines Einkaufs. Ein Nutzer kann dadurch erkennen, wie oft RFID-Marken ausgelesen

[8] § 89 Satz 1 TKG (2004): „Mit einer Funkanlage dürfen Nachrichten, die für (...) nicht bestimmt sind, nicht abgehört werden.“

[9] Vgl. RFID-Marke nach ISO/IEC 15693.

[10] *Bartels/Ahlers*, Gegenspionage – RFID-Detektor im Taschenformat, in c’t 9/2004.

[11] *Flörkemeier* et al., Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols, www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf., schlagen zu diesem Zweck die Einführung einer eindeutigen Reader Policy ID (RPID) vor, die bei Inventory-Anfragen (Auslesen aller RFID-Marken in Reichweite) eines Lesegerätes mitgesendet wird.

bzw. ob Daten auf der Marke verändert wurden.

Ein weiterer Ansatz steuert den Zugriff auf Informationen, die auf einer RFID-Marke gespeichert sind, in Abhängigkeit von der *Entfernung zwischen Marke und Lesegerät*. Ein Lesegerät erhält umso mehr Informationen von einer RFID-Marke, je näher es an der Marke ist.[12] Vorstellbar wäre auch eine Variante, bei der eine RFID-Marke aus großer, nur durch die Reichweite des RFID-Systems beschränkter, Entfernung auslesbar ist, jedoch Schreibzugriffe nur bei sehr geringem Abstand des Lesegerätes zur RFID-Marke zulässt. Schließlich kann das Prinzip der räumlichen Nähe mit kryptografischen Verfahren kombiniert werden. Nur wenn (a) das Lesegerät nah genug an der RFID-Marke ist und (b) eine Authentifizierung erfolgreich war, werden Informationen preisgegeben. Problematisch bei diesem Ansatz ist die Erkennung der Entfernung zwischen RFID-Marke und Lesegerät. Vorgeschlagene Lösungen wie Signalstärkenanalyse, Analyse des Signal-Rauschabstandes oder Triangulation erlauben keine zuverlässige Entfernungsbestimmung.[13]

4.2 Abwehrstrategien gegen Identifizierung

Eine besondere Problemlage entsteht beim Eigentumsübergang von mit RFID-Marken ausgestatteten Produkten, beispielsweise an der Kasse eines Supermarktes. Die RFID-Marke wird nun zur Gefahr für die Privatsphäre des neuen Eigentümers, da er anhand der Markenkennung identifiziert werden kann. Vorstellbar wäre dies durch eine Verknüpfung der Markenkennung mit der Person des Käufers durch ein identifizierendes Bezahlungssystem, zum Beispiel bei Bezahlung mit einer Kundenkarte. Um dieser Gefährdung zu begegnen, wurden bereits verschiedene Verfahren entwickelt.

Mehrere Verfahren stören oder unterbinden ein Auslesen der RFID-Marken durch fremde, d. h. nicht autorisierte Lesegeräte. Das *Jamming* verwendet einen Störsender der die Kommunikation zwischen Lesegerät und RFID-Marke komplett unterbindet. Das *Blocker-Tag* stört diese Kommunikation nur dann, wenn das Lesegerät spezielle, als privat gekennzeichnete, Markenkennungen abfragen will.[14] Im einfachsten Fall könnte der Adressraum von RFID-Marken in eine private und eine öffentliche Zone aufgeteilt sein. Alle privaten RFID-Marken haben eine Kennung beginnend mit einer 0, alle öffentlichen RFID-Markenkennungen beginnen mit einer 1. Sobald ein Lesegerät versucht, im privaten Adressbereich nach RFID-Marken zu suchen, wird das Blocker-Tag aktiv und stört diesen Vorgang, indem es dem Lesegerät vorgaukelt, es wären Millionen von RFID-Marken vorhanden. Das Lesegerät kann daraufhin real vorhandene RFID-Marken nicht mehr erkennen. Beim Eigentumsübergang muss bei diesem Verfahren die Kennung der RFID-Marke angepasst werden. Problem dabei ist, dass eine als privat gekennzeichnete RFID-Marke lediglich die Nutzung durch gewerblich handelnde Lesegerätebenutzer auszuschließen hilft.

Verfahren, die wie beim Jamming oder beim Blocker-Tag die Kommunikation zwischen Lesegerät und RFID-Marke aktiv stören, sind als rechtlich bedenklich einzustufen. Zwar fallen sie nicht unter § 317 Abs. 1 StGB, weil RFID-Systeme nicht Teil des Betriebs öffentlichen Zwecken dienender Telekommunikationsanlagen sind. Sie sind jedoch als Ordnungswidrigkeit nach § 10 Abs. 1 FTEG (wegen § 3 Abs. 2 FTEG) einzuordnen.

Eine zweite Gruppe verändert die Markenkennung beim Eigentumsübergang. Beim *Meta-ID-Verfahren* antwortet die RFID-Marke nach einem Sperrvorgang nicht mehr mit ihrer originären Kennung, sondern mit einer so genannten Meta-ID.[15] Die eigentliche Kennung der RFID Marke erfährt nur derjenige, der den geheimen Schlüssel kennt, mit der die Meta-ID erzeugt wurde, und diesen an die RFID-Marke sendet. Die RFID-Marke bildet aus dem empfangenen Schlüssel die dazugehörige Meta-ID und vergleicht diese mit der gespeicherten Meta-ID. Bei Gleichheit wird die RFID-Marke entsperrt und die Klardaten werden an das Lesegerät übertragen. Dieses Verfahren nutzt das Prinzip der Einweg-Hashfunktionen: Aus dem geheimen Schlüssel lässt sich problemlos die dazugehörige Meta-ID berechnen, es ist jedoch sehr schwierig, aus der Meta-ID den geheimen Schlüssel zu berechnen.

Beim *Kill-Tag*-Ansatz[16] wird die RFID-Marke durch einen speziellen Befehl des Lesegerätes komplett und unwiederbringlich deaktiviert. Problematisch wird dieses Verfahren, wenn der Kunde einen gekauften Artikel wieder in den Laden zurückbringt. Der Artikel muss dann wieder in das Warenwirtschaftssystem eingegliedert werden, wozu das Anbringen einer neuen Marke erforderlich wäre. Der Artikel erhielte dann praktisch eine neue Identität. Zwar ist für die Abwicklung von Gewährleistungsansprüchen der Zugriff auf Informationen der „vergangenen" Identität des Warenartikels nicht erforderlich, jedoch kann der Käufer eines Warenartikels mit deaktivierter RFID-Marke den Mehrwert dieses Kennzeichnungsverfahrens nicht für private Zwecke nutzen. Der „intelligente Kühlschrank" würde dann nicht mehr funktionieren.

4.3 Technische Gestaltungsvorschläge

Wir schlagen als Gestaltungsidee einen *modifizierten Kill-Befehl* vor, der anders als das bisherige Verfahren nicht die komplette Markenkennung löscht, sondern nur den eindeutig identifizierenden Teil dieser Kennung. Die eindeutige Seriennummer eines Artikels wird gelöscht oder gegebenenfalls durch eine private Inventarnummer ersetzt, die Objektklasse des Artikels bleibt jedoch erhalten. Dies beschränkt die Aussagekraft der RFID-Marke auf die eines Barcodes. Beim EPC (Electronic Product Code) setzt sich eine Kennung nach SGTIN-96 (Serialized Global Trade Identification Number) unter anderem aus einer Herstellerkennung (Company Prefix), einer Artikelreferenz (Item Reference) und einer 38-bit langen Seriennummer zusammen. Unser Ansatz deaktiviert die Seriennummer; Herstellerkennung und Artikelreferenz (Objektklasse) bleiben erhalten. Damit lassen sich RFID-Marken auch nach dem Kauf nutzen.

Ein zweiter Gestaltungsvorschlag betrifft die Infrastruktur eines serverbasierten, überregional vernetzten RFID-Systems, wie es vom EPCglobal-Konsortium vorgeschlagen wird.[17] Dabei geht es um die Auflösung des

[12] Technisch umsetzbar wäre dies durch die Verwendung von Übertragungsverfahren unterschiedlicher Reichweite.

[13] *Fishkin/Roy*, Enhancing RFID Privacy via Antenna Energy Analysis, Proc. of MIT RFID Privacy Workshop, Boston, November 2003.

[14] S. zu beiden *Juels/Rivest/Szydlo*, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, in: Atluri (Ed.), Proc. of the 8th ACM Conference on Computer and Communications Security, 2003, 103-111.

[15] S. *Sarma/Weis/Engels*, RFID systems and security and privacy implications, in: Kaliski/Co/Paar (Ed.), Cryptographic Hardware and Embedded Systems – CHES 2002, 454-469.

[16] S. dazu EPC Version 1.0/1.1 Specification.

[17] S. dazu EPC Version 1.0/1.1 Specification.

Zusammenhangs zwischen RFID-Marke und eindeutig identifizierbarem Gegenstand. Eine RFID-Marke speichert eine Objektidentität gewöhnlich als Bit-Serie, beim EPC zum Beispiel mit einer Länge von 64 oder 96 bit. Die wahre Identität und ein möglicher Personenbezug lassen sich jedoch erst nach einer Decodierung dieser Bitserie herstellen. Dies geschieht beim EPC durch Anfrage bei einem ONS-Server, der Zugriff auf eine verteilte Datenbank hat, die zu einer EPC-Nummer weiterführende Informationen abspeichert. Ein ONS-Server kann überdies zur Aufzeichnung eines Bewegungsprofils verwendet werden, indem er Orte und Zeiten von Auslesevorgängen einer RFID-Marke protokolliert.

Wir schlagen eine auf § 35 Abs. 2 bis Abs. 5 BDSG gestützte Löschung, hilfsweise Sperrung des ONS-Eintrages (oder des Eintrages in einer vergleichbaren Datenbank eines anderen Systems) vor, um die Privatsphäre des Eigentümers eines Produktes mit RFID-Marke besser zu schützen. Es lässt sich zwar weiterhin die RFID-Marke mit jedem Lesegerät auslesen, personenbezogene Daten können damit jedoch nicht erlangt werden.

Alternativ könnte beim Eigentumsübergang eines Produktes auf dem Speicher der RFID-Marke ein Löschungsbit gesetzt werden. Registriert ein Lesegerät, das an das EPCglobal-Netzwerk angeschlossen ist, dieses Bit, so wird eine Löschung (Sperrung) des ONS-Eintrages veranlasst.

Überdies könnte eine Zugangsbeschränkung zum ONS-System eingeführt werden. Es kann dann zwar jeder eine Anfrage stellen, Antworten erhält jedoch nur, wer sich vorher als berechtigt authentifiziert hat.

Kennzeichnung der Zielanwendung

Wie kann ein Lesegerät erkennen, für welche Anwendung eine bestimmte RFID-Marke arbeitet? Eine Waschmaschine, die ihr Waschprogramm anhand der erkannten RFID-Marken der in ihr enthaltenen Kleidungsstücke auswählt, sollte auch nur diejenigen Marken auslesen, die zu dieser speziellen Anwendung gehören. Wir schlagen dafür die Einführung einer Anwendungskennung (AK) vor, für die ein Speicherabschnitt auf der RFID-Marke reserviert ist. Dabei wird gefordert, dass eine Anfrage des Lesegerätes immer in Kombination mit einer AK ausgesendet werden muss, die genau eine Anwendung spezifiziert. Eine RFID-Marke antwortet nur dann auf die Anfrage des Lesegerätes, wenn dessen AK mit der eigenen Anwendungskennung übereinstimmt. Dies erfordert implizit, dass auf einer RFID-Marke gegebenenfalls Platz für mehrere Anwendungskennungen reserviert werden muss, wenn der damit verbundene Artikel in mehreren Anwendungen eingesetzt werden kann. Die Anwendungskennung sollte vom Nutzer gegen Änderungen gesperrt werden können. Ein Entsperren sollte nur mittels eines geheimen Schlüssels möglich sein.

Ein ähnliches Verfahren ist bereits in ISO/IEC 15693[18] spezifiziert. Dort ist jede Marke mit einer AFI (Application Family Identifier) ausgestattet. Das Lesegerät sendet eine AFI zusammen mit dem Inventory-Befehl. Dieses mit einer AFI versehene Kommando lässt nur die RFID-Marken in der Umgebung antworten, die die gleiche AFI haben. Marken mit ungleicher AFI bleiben hingegen stumm.

Die ISO/IEC 15693 spezifiziert weiterhin, dass eine Anfrage des Lesegerätes ohne AFI von allen RFID-Marken beantwortet werden muss. Wir fordern dagegen, dass jede Anfrage eines Lesegerätes mit einer AFI versehen werden muss. Andernfalls darf keine der vorhandenen RFID-Marken antworten.

Kennzeichnung des Verwendungszwecks

Wie kann ein Lesegerät erkennen, für welchen Zweck die Daten auf einer RFID-Marke bestimmt sind? Angenommen, die Kennung der RFID-Marke ist nur bedingt aussagekräftig und mit ihr allein ist kein Personenbezug herstellbar. Weiterhin nehmen wir an, dass nur, wenn neben der Kennung auch der sonstige Speicher auf der RFID-Marke ausgelesen wird, ein Datenschutz-Problem entstehen kann. Wir schlagen für diesen Fall die Einführung einer Verwendungskennung (VK) vor. Wie die Anwendungskennung ist auch die VK auf der RFID-Marke gespeichert und kann gegen Veränderung gesperrt werden. Das Lesegerät fragt RFID-Marken in der gewohnten Weise ab. Die RFID-Marken antworten mit ihrer Markenkennung und der VK. Die VK spezifiziert dabei die Möglichkeit der Verwendung der Daten, womit eine Zweckbindung von RFID-Daten erreicht werden kann. So können beispielsweise gewerbliche Daten eine andere VK haben als private Daten. Ein Lesegerät erfährt dadurch zunächst nur die Markenkennung und den Verwendungszweck der auf der RFID-Marke gespeicherten sonstigen Daten. Diese sonstigen Daten sollten nur dann ausgelesen werden, wenn sie für den Zweck, den das Lesegerät vertritt, gedacht sind.

Eine ähnliche Kennung ist in der ISO/IEC 15693 spezifiziert. Der darin beschriebene DSFID (Data Storage Format Identifier) arbeitet ähnlich wie die VK, spezifiziert jedoch nicht den Verwendungszweck der Daten, sondern deren Speicherformat.

5 Fazit und Ausblick

Bei den präsentierten Gestaltungsvorschlägen ist zu berücksichtigen, dass für RFID-Systeme kein einheitlicher Standard existiert. Vielmehr gibt es viele Normen und Standards mit unterschiedlichen Charakteristika und Einsatzzwecken.[19] Die präsentierten Gestaltungsideen sind möglichst generisch verfasst und sollen als Grundstein für eine derzeit noch hypothetische Meta-Norm für alle RFID-Systeme dienen, die Problembereiche für die Wahrung des Fernmeldegeheimnisses und der informationellen Selbstbestimmung berühren.[20]

Es ist zu erwarten, dass sich die angesprochenen Probleme auf Grund des technischen Fortschritts und damit einhergehender Zunahme der Speicher- und Rechenkapazität von RFID-Marken weiter verschärfen werden. Fortschritte in der Mikrosystemtechnik versprechen außerdem eine Integration von Sensoren auf RFID-Marken, so dass diese in der Lage sein werden, Umgebungsinformationen selbständig aufzunehmen und zu speichern.

Um in einer zunehmend informatisierten Welt konsentierte zivilisatorische Errungenschaften, die in Grundrechte gefasst sind, zu erhalten, bedarf es neben einer Fortentwicklung des (Datenschutz-)Rechts[21] auch einer vorsorgenden technischen Gestaltung. Nur in einer Kombination von Recht und Technik werden die beschriebenen Risiken zu bewältigen sein.

[18] Norm für kontaktlose Identifikationskarten.

[19] Für Logistikanwendungen u. a. ISO/IEC 18000, 15961-15963, 15418; für kontaktlose Identifikationskarten ISO/IEC 10373, 10536, 14443, 15693 .

[20] Zuständig dafür wären Normierungsgremien wie die International Electrotechnical Commission (IEC) oder die International Organisation for Standardization (ISO).

[21] S. z. B. *Roßnagel/Müller*, Ubiquitous Computing – Neue Herausforderungen für den Datenschutz, CR 2004, 617 ff.