Frank Seeliger, Frank Gillert,
Cliff Buschhart (Hrsg.)

RFID für Bibliothekare: ein Vademecum

Technische
Hochschule
Wildau [FH]
Technical University
of Applied Sciences

WILDAU

Verlag News & Media

Autoren

Marco Althaus
Anke Berghaus-Sprengel
Josef Bernhard
Daniel Büth
Catherine Cooke
Tobias Dräger
Olaf Eigenbrodt
Achim Enders
Frank Gillert
Michał Grabia
Dieter Horst
Tomasz Janiak
Christian Kern
Guido Kippelt
Jan Kissig
Doris Köhler
Sebastian Krautz
Marian Margraf
Wolfgang Meißner
Barbara Michaelis
Ulrich Naumann
Cathrin Neumair
Rainer Sprengel
Ulrike Verch
Markus Weinländer
Hardy Zissel

ISBN 978-3-936527-32-2
Verlag News & Media

Frank Seeliger, Frank Gillert, Cliff Buschhart (Hrsg.)

RFID für Bibliothekare: ein Vademecum

Technische
Hochschule
Wildau [FH]
Technical University
of Applied Sciences

WILDAU

Bibliographische Information der Deutschen Bibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.ddb.de abrufbar.

»RFID für Bibliothekare: ein Vademecum«, herausgegeben von Frank Seeliger, Frank Gillert und Cliff Buschhart im Auftrag des Präsidenten der Technischen Hochschule Wildau [FH], Prof. Dr. László Ungvári

ISBN 978-3-936527-32-2

3. Auflage, Juni 2014

Gesamtherstellung: News & Media, Berlin
www.newsmedia.de
Printed in Germany

Inhalt

Vorwort

Vor sechs Jahren fand das erste zweitägige RFID-Symposium in Wildau statt, schon ein Jahr später, nach dem zweiten Symposium, war der Wunsch gereift, im Rahmen einer ersten Aufsatzsammlung auf dieser Konferenz vorgetragene Themen publizistisch aufzubereiten. Die Beiträge, so der auch oft an die Herausgeber herangetragene Wunsch, sollten erläuternder sein, als die verfügbaren online-Präsentationen,[1] somit auch denen verständlich, welche nicht an den RFID-Symposien teilnehmen konnten.

Nach dem fünften RFID-Symposium und drei Jahren der sammelnden Tätigkeit ist es uns, den beiden Herausgebern, gelungen, aus den ca. achtzig mittlerweile gehaltenen Konferenzbeiträgen und solchen, die im kommenden Jahr das Programm der Konferenz bereichern sollen, diejenigen für diese Kompilaton auszuwählen, deren Relevanz über den Einzelfall hinaus gegeben ist, ganz in Horaz' Sinne: *tua res agitur* (es handelt sich um Deine Sache).

Die thematische Spannweite ist dabei sehr groß und könnte sogar unter Anspielung auf einen alten Filmtitel etwas erweitert werden zu dem Motto: Was Sie schon immer über RFID wissen wollten und sollten, aber bisher nicht zu fragen wagten oder zu fragen gedachten!

Bei der thematischen Auswahl floss neben Horaz' Anspruch ebenfalls mit ein, dass im letzten Jahr (2011) beim renommierten Springer-Verlag von Christian Kern das sehr informative und zu empfehlende deutschsprachige Handbuch »RFID für Bibliotheken« erschienen ist, welches mit aller notwendigen Expertise bereits ausführlich auf die Physik und Technik der Funktechnologie eingeht, umfänglich Themen wie Ausschreibung, Konvertierung, einzelne RFID-Geräte etc. behandelt. Vor diesem Hintergrund soll das vorliegende Werk den Blickwinkel auf die hier im Mittelpunkt stehende Technologie ergänzen und erweitern, und gegebenenfalls zur Diskussion anregen.

Die im vorliegenden Nachschlagewerk enthaltenen Beiträge greifen Themen wie das Innovationspotenzial, Lobbyarbeit, wirtschaftliche Aspekte, die Entwicklung der Bibliothekstechnik generell auf, nehmen sich aber auch rechtlicher Aspekte an, den Inventurverfahren, möglicher gesundheitlicher Gefährdungen, der Qualität und den Standards, den zwei gängigen Schnittstellen zum Bibliotheksmanagementsystem, den bauphysikalischen Aspekte, verschiedenen Betrachtungswinkeln auf den Logistikkreislauf, Problemfeldern von Fernleihe bis NFC-befähigten Smartphones, weiteren Features etc.

Es ist kurzum ein bunter Blumenstrauß, der sich bei dieser Thematik, RFID, zwangsläufig ergeben muss, da ungemein viele Aspekte ein Projekt berühren, welches die Einführung, Unterhaltung oder Weiterentwicklung von RFID-Technologie im Bibliotheksumfeld zum Ziel hat. Insofern stellt diese Projektarbeit oder ins Tagewerk einfließende Aufgabe eine nicht zu unterschätzende Herausforderung für den damit beauftragten und

1 siehe http://www.th-wildau.de/hochschule/einrichtungen/bibliothek/die-bibliothek-vor-ort/veranstaltungen-events/rfid-symposien.html

beschäftigten Bibliothekar dar. Die KollegInnen in diesem Aufgabenbereich zu unterstützen, ist das erste Ziel des vorliegenden Bandes. Und derer, die im Berufsalltag damit konfrontiert sind, werden es zunehmend mehr, da die Einführung von RFID-Technologie in Bibliotheken und Informationseinrichtungen ein rasantes Tempo annimmt. Bedenkt man, dass vor knapp fünfzehn Jahren die erste Bibliothek in Singapur diese Technik einführte, vor zehn Jahren die erste in Deutschland, so liegen die Schätzungen heutigentags bei eintausend Installationen (mit Zweigstellen) hierzulande und weltweit um eine Potenz höher.

Es ist bei dieser Menge an RFID-Implementierungen und darin involvierten BibliothekarInnen, die keine *Quantité négligeable* darstellen, fast schon verwunderlich, wie stiefmütterlich und zurückhaltend das Thema bei einschlägigen Publikationskanälen und Fachdiskussionen nicht nur hierzulande behandelt wird. Vom »smattering use« (halbwissenden Umgang) ist auf Tagungen wie den Jahreskonferenzen der IFLA immer wieder die Rede. Laut Aussagen des britischen Mr. RFID, Mick Fortune, und nach Auswertung der ersten globalen Umfrage von RFID-Anwendern in der Bibliothekswelt[2] setzen viele KollegInnen RFID ausschließlich mit »selfcheck« bzw. Selbstverbuchung gleich. Die Funktechnologie greift mit den klassischen Anwendungsfeldern Sicherung und Selbstverbuchung umfassend in den Bibliotheksalltag ein, birgt ein noch nicht ausgeschöpftes Potential in sich, erlangt aber dennoch nicht die Aufmerksamkeit wie andere Initiativen und Themenfelder im Bibliothekskontext. Vielleicht gelingt es mit dieser Kompilation an Beiträgen nicht nur das allgemeine und vertiefende Interesse in der eigenen Zunft zu wecken, sondern ebenfalls ein Engagement entfalten zu lassen, welches der RFID-Technologie den Auftrieb gibt, mehr noch als bislang bei Automatisierungen, Serviceleistungen am Kunden, dem Sicherheitsbedürfnis und neuen Diensten in den Informationseinrichtungen sich einzubringen und mit zu gestalten.

Das primäre Ziel jedoch dieses Bandes ist es, der oder dem mit Funketiketten, RFID-Selbstverbuchern und Schleusen beschäftigten Kollegin oder Kollegen, ein unentbehrlicher Begleiter, ein Vademecum, zu sein.

In diesem Sinne wünschen Ihnen eine anregende Lektüre

Frank Seeliger, Frank Gillert und Cliff Buschhart

2 siehe http://www.libraryrfid.co.uk/2012.html

Vom Lochstreifen zur berührungslosen Kommunikation

Persönliche Eindrücke aus der Technikgeschichte der Bibliotheken

Ulrich Naumann

Ich habe vor vielen Jahren meine Ausbildung in der damaligen Stadt- und Universitätsbibliothek Frankfurt am Main unter der Leitung von Clemens Köttelwesch begonnen. Köttelwesch hatte zehn Jahre zuvor (ich spreche vom Jahr 1964) einen innovativen Bibliotheksbau errichtet, voll mit neuen konzeptionellen Ideen der Bestandsdarbietung: 750.000 Bänden als Freihandbestand, 1000 Benutzerarbeitsplätze auf vier Fachebenen. Und dennoch vertrat dieser bedeutende Bibliothekar die Auffassung (ich zitiere):

»Es sei darum hier nur die selbstverständliche Bemerkung erlaubt, daß wir alle technischen Einrichtungen, die zur Beschleunigung und Intensivierung der anfallenden Arbeit beitragen können, im neuen Gebäude gern nutzen werden, wenn wir sie ausfindig machen können und wenn sie ausreichend erprobt sind.«[1]

Und so habe ich dann 1974 meine Ausbildung zum Bibliothekar in Frankfurt am Main begonnen, bewaffnet mit einer Typenhebelschreibmaschine zum Anfertigen der Katalogkarten. Immerhin werden sie im Achternutzen auf Kunststoff-Matrizen geschrieben und dann für die zahlreichen Zettelkataloge in verschiedenen Kartonfarben vervielfältigt.

Als ich dann 1976 den Auftrag erhielt, die Hessische Bibliographie auf eine neue Basis zu stellen, wurde dabei festgelegt, dass die gedruckten Bände mit Hilfe der Gesellschaft für Information und Dokumentation (GID) auf EDV-Basis hergestellt werden sollten. So habe ich unsere Erfassungsbögen zu einem benachbarten Erfassungsbüro getragen, wo die Daten unter ungeheurem Geratter mit Lochstreifenschreibmaschinen erfasst und in den Großrechner der GID eingelesen wurden. Kamen neben den Erfassungskorrekturen, die vom Büro erledigt werden mussten, weitere Korrekturen hinzu, bin ich mit der Straßenbahn von der Bockenheimer Warte nach Frankfurt-Niederrad zur GID gefahren und habe diese Korrekturen mit einer Lochstreifenschreibmaschine erfasst. Dabei war genau anzugeben, in welcher Zeile bei welchem Wort der wievielte Buchstabe zu ersetzen war. Diesen Code hatte ich mir vorher beim Korrekturlesen auf Karteikarten notiert, in die richtige Reihenfolge gebracht und diese Karteikarten abgetippt. Mein Lochstreifen wurde dann mit dem vorhandenen Lochstreifen zu einem neuen Lochstreifen vermischt. Der Ausdruck erfolgte zunächst auf Klarsicht-Folien, die nach dem abschließenden Korrekturbetrachten (bei über 800 Seiten konnte man nicht mehr vom Korrekturlesen

1 Köttelwesch, Clemens: Zum Neubau der Stadt- und Universitätsbibliothek Frankfurt am Main. In: Buch und Welt: Festschrift für Gustav Hofmann zum 65. Geburtstag dargebracht. Wiesbaden: Harrassowitz, 1965, S. 128.

sprechen) dem Drucker übergeben wurden, der den jeweiligen Band der Hessischen Bibliographie im Offset-Druck produzierte. Ich hatte damals zwar eine dunkle Ahnung, dass man das Produktionsverfahren auch technisch eleganter hätte lösen können, aber erst nach meinem Weggang aus Frankfurt 1982 wurden erste zögernde Schritte in Richtung bildschirmgestützte Erfassung und Korrektur eingeleitet. Unser damaliger stellvertretender Direktor Klaus-Dieter Lehmann, heute Präsident des Goethe-Instituts, war da schon weiter: Er beriet damals ein kleines Startup-Unternehmen der Jerusalemer Universität bei bibliothekarischen Anwendungen. Ich spreche von der Fa. ExLibris.

In Berlin, wohin ich 1982 gewechselt habe, stand ein Fernschreiber zur Verfügung, mit dem wir den Fernleihbetrieb mit der Staatsbibliothek in Berlin rationalisiert haben. Es gab auch eine Recherchestation für die Informationsvermittlung. Sie wurde von den Fachreferenten benutzt, weil die unterschiedlichen Retrievalsprachen in den verschiedenen auf Großrechner gelagerten Datenbanken eine große Bedienungskompetenz erforderten (ich erinnere Eingeweihte nur an GRIPS/DIRS, mit der DIMDI-Datenbanken durchsucht werden konnten, oder GOLEM und STAIRS)[2]. Das dazu notwendige Telefon wurde mit einem Einmachglas-Gummi unverrückbar mit dem Modem verbunden. Der dafür benutzte Computer kostete 18.000 DM, wir hatten ihn für 3.000 DM im Jahr gemietet. 1986 habe ich ihn dann für einen Restwert von 3.000 DM gekauft, um die jährlichen Mietzahlungen zu sparen.

Auf dieser Maschine habe ich dann 1984 unter Anleitung unseres Referendars Marcel Brannemann, einem echten Computer-Freak, auch meine erste eigene Bibliographie produziert. Hierbei hatte ich immer zu beachten, dass nicht benötigte Dateien auf der immerhin insgesamt 10 Megabyte umfassenden Festplatte gelegentlich auf 5 ¼-Zoll-Disketten ausgelagert werden mussten, um weiterarbeiten zu können. Der Rechner selbst lief unter dem Betriebssystem C/PM86.

Meine Kollegin Dorothea Reinhold, die mit demselben Elan an einer Meta-Bibliographie für die Geschichte Berlin und der Mark Brandenburg arbeitete, schrieb 1986 in ihrem Vorwort:

»Die kleine Veröffentlichung entstand aus einem allgemeinen Interesse an Regionalbibliographie und Landesgeschichte und auch aus Neugierde. Die Neugierde galt der Frage, was man mit einem Personalcomputer, – er führt häufig noch ein Schattendasein in vielen großen Bibliotheken -, und etwas Datenbanksoftware (dBase II) mit minimalen Textverarbeitungsmöglichkeiten bibliographisch leisten kann.«[3]

---

2 GRIPS/DIRS (General Relation Based Information Processing System/Document Information Retrieval System) ist der Name einer Retrievalsystemsoftware des Deutschen Instituts für medizinische Dokumentation und Information (DIMDI), die auch Programme für Datenbankaufbau und -pflege beinhaltet.
Andere Sprachen: GOLEM (Großrecherorientierte, listenorganisierte Ermittlungsmethode) von Siemens. Es wurde für die olympischen Spiele 1972 in München entwickelt. Das System GOLEM wurde konzipiert für unformatierte Daten und Texte, bei denen der Zugriff über Deskriptoren und invertierte Listen erfolgte. STAIRS (Storage and Information Retrieval System) ist das Softwarepaket der Firma IBM für das Information Retrieval, das 1969 entwickelt wurde. Es ist, ebenso wie GOLEM, teilweise heute noch im Einsatz, arbeitet partiell menüorientiert und besitzt bereits komfortable Retrievalmechanismen wie adjacency-Suche (Abstandsoperatoren) und Ranking-Algorithmen.

3 Reinhold, Dorothea: Bibliographien zur Geschichte und Landeskunde Berlins und der Mark Brandenburg. Berlin: UB der FU Berlin, 1986, S. III.

1995 haben wir wieder das große Engagement unserer damaligen Referendarin Dr. Sybilla Prochitzki, die vom französischen CNRS kam, genutzt, um einen Internet-Auftritt unserer Bibliothek dauerhaft zu organisieren. Wir lernten alle HTML, um uns in der für uns neuen Welt zu bewegen, und bekamen Anregungen, wie wir dieses Instrument INTERNET in unsere Arbeit einbinden konnten.

Es wird deutlich geworden sein, dass nicht nur das Technologie-Angebot, sondern vor allem personelle Glücksfälle und die Bereitschaft der Mitarbeiterinnen und Mitarbeiter, die gewohnten Pfade zu verlassen und Neues auszuprobieren, ein wesentliches Moment für die Einführung neuer Technologien in Bibliotheken sind. Hierbei sollte immer auch mitgedacht werden, dass Bibliotheken lebendige soziale Gebilde aus Mitarbeitenden und Nutzenden sind, die sich ab einer bestimmten Größe nicht mehr für Laborexperimente eignen. Zum Glück werden wenigstens die Benutzer einer wissenschaftlichen Bibliothek in einem überschaubaren Zeitraum von 3 bis 5 Jahren fast komplett ausgetauscht, so dass hier Neuerungen eher evolutionär als revolutionär erscheinen.

Ähnliches Spannendes, dann aber auch Langatmiges könnte ich Ihnen von unserer Ausleihe berichten, bei der wir bereits in den siebziger Jahren in einem überschaubaren Bereich, der Lehrbuchsammlung, mit der Lochkartenverarbeitung in der Verbuchung begonnen haben. 1984 wurde in der Hauptausleihe ein OCB-B-gestütztes BIAS-System eingerichtet. Die Lehrbuchsammlung folgte erst ein Jahr später, nachdem sich für die dortigen Mitarbeiter (man denke an die Abteilungszäune selbst in einer Benutzungsabteilung) die Funktionsfähigkeit in der Hauptausleihe ohne die geliebten Lochkarten erwiesen hatte. Den Übergang zum neuen System einfach anzuordnen war aus psychologischen Gründen nicht zweckmäßig. In der Psychologie spricht man von einem reaktanten Verhalten: Verbiete dem Mitarbeiter, ein bestimmtes System zu nutzen, und er wird alles daran setzen, es zu nutzen, auch wenn er es vorher vehement abgelehnt hat.

In der Zugangsbearbeitung haben wir nach einigen Geburtswehen erst 1990 begonnen, unsere Titelaufnahmen in den Berliner Katalogisierungsverbund IBAS einzubringen. Für unser Haus war das, wie ich es einmal formuliert habe, ein Umstieg von der Steinzeit in das Raketenzeitalter. Bis dahin hatten unsere Titelaufnehmerinnen in einem stillen größeren Büro die Titelaufnahmen in einem vereinfachten Verfahren mit weichem, nicht kratzenden Bleistift vorgeschrieben. Die Titelaufnahmen wurden dann von räumlich entfernten Hilfstitelaufnehmerinnen mit der Schreibmaschine auf Titelkarten übertragen und maschinell vervielfältigt. Unsere Benutzer haben wir über die Erfolge in unserer elektronischen Verarbeitung der Titelaufnahmen mit immer größer werdenden formal und sachlich geordneten Mikrofichekatalogen informiert. In der Erwerbungsabteilung hat sich das manuelle Verfahren mit Sortierung nach den Preußischen Instruktionen bis 1999 gehalten.

Erst mit der Jahrtausendwende, als wir gezwungen waren, wegen der Jahr 2000-Problematik (Y2K-Problematik =»Year 2 Kilo«) das Siemens-System BIAS zu wechseln, wurde mit dem Übergang auf das ALEPH-System das erste integriert arbeitende Bibliotheksinformationssystem eingerichtet, zu dem nun auch die Benutzer Zugang hatten. Das ist nun gerade 11 Jahre und sechs Versionen dieses Systems her.

Wenn man sich in den Berichten anderer großer Bibliotheken umschaut, erkennt man, dass wir an der Freien Universität Berlin keineswegs das Schlusslicht einer rasanten Entwicklung gewesen sind, auch wenn wir uns nicht an vorderster Front durch ein großes Innovationsstreben ausgezeichnet haben. Das mag auch an der Größe unseres Bibliothekssystems liegen, wo wir mit 8,5 Mio. Bestandseinheiten immer noch eine Spitzenposition in Deutschland einnehmen, aber auch bei umfassenden technischen Innovationen auf unsere etwa 50 relativ autonom agierenden Fachbibliotheken Rücksicht müssen.

In der jüngeren Technik-Geschichte unserer Bibliotheken und in der Technik-Gegenwart sind noch keine klaren Linien zu erkennen, die man mit einigen Worten plakativ beschreiben könnte. Zuviel tut sich an vielen Fronten, und es ist nicht ganz leicht, eine große strategische Linie als das Systemische unseres Handelns zu definieren. Hierbei zeigt z. B. ein Bericht des Stuttgarter Hochschul-Kollegen Martin Götz, was alles an technologischen Neuerungen möglich und einsetzbar ist.[4] Lassen Sie mich dazu einige Überlegungen vortragen.

Denken wir unter anderem an die Frage, was eigentlich unser Katalog ist. Früher war das relativ leicht damit zu beantworten, dass der Katalog alles enthält, was wir in der Bibliothek an physischen Beständen anzubieten haben. Bleibt man bei dieser Definition für den eigenen Katalog, muss akzeptiert werden, dass der Katalog heute nur noch einen Ausschnitt dessen bietet, was wir an Informationspotenzial für unsere Benutzer bereitstellen. Die Hunderttausende elektronisch verfügbarer Volltexte und Datenbanken, zu denen wir mit unseren Systemen den Zugang ermöglichen, werden vom Benutzer als unser Bibliotheksangebot wahrgenommen. Die Frage, ob wir dafür auch den physischen Besitz in Print- oder digitalisierter Form haben, ist für ihn absolut nachrangig. Daher ist es eine nicht ganz leichte Aufgabe, diesen Bestandskatalog in eine umfassendere Informationswelt zu integrieren. Für unser Bibliotheksinformationssystem ist mit der ALEPH-Software PRIMO eine solche »one-stop-agency« geschaffen worden, die die durch GOOGLE sozialisierten Benutzerinnen und Benutzer zu Recht erwarten können. Natürlich sind unsere Informationen auch auf heimischen Rechnern und den sog. mobile devices wie Smartphone, iPhone und iPad nutzbar und öffnen das Bibliotheksangebot in die reale und zugleich virtuelle Welt.

Welche Blüten solche Technologie hervorbringen kann, zeigt das Beispiel der Bayerischen Staatsbibliothek, die 20 digitalisierte Spitzenwerke des islamischen Kulturkreises ausschließlich für das iPhone und das iPad aufbereitet hat und als Application über iTunes bereitstellt. Ich möchte bezweifeln, dass sich die feinen Miniaturen dieser Spitzenwerke auf dem 9 cm großen iPhone-Bildschirm sehr gut erkennen lassen.

Ähnliche Entwicklungen für unser Informationsangebot können im Bereich der Medienerwerbung festgestellt werden. Früher haben wir ein Medium gekauft und in unseren Bestand übernommen. Streit gab es nur bei der Lehrbuchsammlung, wo zu Lasten des dauerhaften Medienerwerbs Verbrauchsexemplare mit einer begrenzten Verweildauer

4 S. Götz, Martin: »Technik in Bibliotheken«, B.I.T.online 12 (2009), Nr. 1, S. 51-59 (Überblickartikel, in dem er »die wichtigsten einzusetzenden und eingesetzten Techniken in Bibliotheken und ihre zum Teil jetzt schon absehbaren Folgen« behandelt.

beschafft wurden. Aber das war bei uns letztlich Spiegelfechterei bei einer Finanzausstattung, die mehrere Millionen DM und dann auch mehrere Millionen Euro für den Medienerwerb vorsah.

Heute stellt sich die Situation jedoch erheblich anders dar. Inzwischen geben wir über 50 % unseres Etats, der seit Jahren nicht gewachsen ist, für Nicht-Greifbares aus, nämlich Lizenzen für Datenbanken und zugekaufte E-Medien. Diese erfordern wiederum eine ganz andere bibliothekarische Verwaltung, weil es dabei kaum abgeschlossene Erwerbungsprozesse gibt, sondern mit schöner Regelmäßigkeit neue Entscheidungen über den Weiterbezug, also den Abschluss neuer Lizenzen, zu treffen sind. Allerdings hat dies auch Vorteile: Medienpakete, die nachweisbar nicht genutzt werden, werden wieder aufgegeben und damit die Mittel wieder frei. Bei unseren nicht benutzten Print-Medien – und ca. 70 % unseres Bestandes zählt zum aktuell nicht nachgefragten – hilft nur die physische Vernichtung, um Platz für Neues zu schaffen. Auch der Einkauf von E-Book-Paketen hat dabei so seine Tücken hinsichtlich der formalen Erschließung und der Präsentation. Das hat auch nachhaltige Auswirkungen auf unsere Mitarbeiterinnen und Mitarbeiter. Sie müssen alte Qualifikationen über Bord werfen und sich mit neuen Technologien und Verfahrensweisen vertraut machen. Das fällt nicht immer leicht und verstärkt den Anpassungsdruck.

Und eine andere Gruppe unserer Mitarbeiterinnen und Mitarbeiter gewinnt immer mehr Bedeutung für einen reibungslosen Betriebsablauf, die wir erst allmählich aus dem vorhandenen Personal aufbauen mussten bzw. durch Stellenumwandlung von Bibliotheksstellen einstellen konnten: unser EDV-Personal. Diese Mitarbeiter – und sicherlich sind auch viele dieser Gruppe hier vertreten – sind eine interne Dienstleistungsgruppe innerhalb unserer Dienstleistungsorganisation. Das mit der internen Dienstleistung für unsere Bibliothek ist nicht immer zu vermitteln und führt auch zu Reibereien, die oftmals an die Diskussion über das Huhn und das Ei erinnern. Das Tun der EDV-Leute ist manchmal nicht durchschaubar, die Festlegungen für einen aus EDV-Sicht zu organisierenden Betrieb sind nicht immer bibliothekspolitisch nachvollziehbar, und sie haben mit ihrer Kompetenz und ihrem Fachwissen eine gewisse Machtposition, die auch durch die formale Leitungskompetenz eines Direktors nicht immer aufgehoben werden kann – es sei denn, er ist selber EDV-Spezialist, dem man kein X als ein U verkaufen kann.

Was soll ich armer Direktor denn entgegnen, wenn aus der EDV-Abteilung die Forderung erhoben wird, nach knapp vier Jahren schon wieder einen neuen Server für 100.000 Euro zu beschaffen, weil der alte Server –»der ja eigentlich in das Deutsche Technikmuseum Berlin gehört« – nicht mehr performant genug ist. Prüfen kann ich es nicht, die Performanzschwierigkeiten liegen sicherlich im oberen Sekundenbereich, aber unter einer Minute, also schreibe ich – nicht vollständig von der Dringlichkeit überzeugt – einen Bettelbrief an meinen Kanzler mit der Bitte um zentrale Mittel, immer mit dem gewichtigen Argument verbunden, dass er sonst die Literaturversorgung der Universität gefährdet.

Am deutlichsten ist die Veränderung unserer Arbeitswelt in Richtung auf berührungslose Kommunikation aber im Bereich der Benutzung zu sehen. Auf den Wildauer Symposien

ist eine spezielle Anwendung – die RFID-Technologie – bestimmendes Thema. Aber auch andere technologisch gestützte Verfahren greifen immer mehr in unsere Beziehungen zu den Benutzerinnen und Benutzern ein. Hierbei machen wir uns selbst teilweise überflüssig, indem wir die Prozesse nur noch aus dem Hintergrund steuern, und das »wir« müssen keine Bibliothekare sein. Gerade die RFID-Technologie macht die Benutzerin, den Benutzer freier und uns an der Benutzungsfront zunehmend überflüssiger.

Wenn wir Bibliotheken als riesige Freihandbibliotheken bauen – und hier ist das Brüder-Grimm-Zentrum in Berlin ein schönes Beispiel – und dann die Medien mit RFID ausstatten, Ausgabe- und Rückgabestationen einbauen, die an automatische Sortieranlagen angeschlossen sind sowie Kassenautomaten zum Gebührenbezahlen daneben stellen – wozu braucht eine solche Self-service-Bibliothek noch die persönlich anwesende Benutzungsbibliothekarin?

Wir beschäftigen uns nunmehr weitgehend kontakt- und berührungslos gegenüber unseren Nutzern mit neuen Produkten und Dienstleistungen im Bereich der Informationsvermittlung wie der digitalen Auskunft in Form von chat bots auf unseren homepages, mit der asynchronen Auskunft über Email und Webformulare, der synchronen Auskunft im Chat-Room, der kooperativen Auskunftserteilung durch mehrere Bibliotheken und der Vermittlung von Informationskompetenz über Schulungen und Web-basierte Tutorials. Vom Bild der bebrillten Bibliothekarin mit Dutt sind wir weg, aber muss es denn gleich ein ätherisch schöner Avatar wie »Stella« in Hamburg sein?

Natürlich liegt einer solchen Bibliothek auch ein Wegweiser-System zugrunde. Der Medien-Standort kann am Bibliotheksrechner und dem Benutzer-Laptop, aber auch mittels des internetfähigen Handys aufgerufen und am Handy-Bildschirm der Weg zum Medium dargestellt werden. Die Bitte, das Handy in der Bibliothek wegen der Störung anderer Benutzer auszuschalten, macht dann wenig Sinn. Auch in den Fußboden eingearbeitete LED-Module, die vom Benutzer angesteuert werden können und ihm individuell den Weg zeigen, sind bereits in der Erprobung.

Wie Frithjof Walk von der Firma Feig Electronic bereits 2007 ausführte, hat der Hype um RFID zu gewaltigen Investitionen in diese Technologie geführt. RFID war bereits ein Verkaufsschlager, bevor RFID-Technologie richtig verkauft wurde. Nun muss sie aber auch verkauft werden. Gelegentlich werde ich an Clemens Köttelwesch erinnert, den ich eingangs zitierte und dessen abwartende Haltung bei dem Einsatz von Technik bei manchem Progressiven auch unter Ihnen ein Lächeln ausgelöst hat. Wir stehen z. B. gegenwärtig vor der Entscheidung, ob wir eine neue große Freihandbibliothek mit 1,2 Mio. Bestand mit einem RFID-System auf HF- oder UHF-Basis ausrüsten. Diese Problematik war auch schon Gegenstand beim 2. Wildauer Symposium vor zwei Jahren, wo auf der Agenda neben Fragestellungen zu den optimalen Schnittstellen zwischen RFID-Komponenten und dem verwaltenden Bibliothekssystem (SIP2, NCIP) die alternativen Frequenzbereiche (HF versus UHF) behandelt wurden.

Sollen wir es mit Köttelwesch halten und auf die in Bibliotheken bewährte HF-Technologie setzen oder sollen wir es riskieren, die in Bibliotheken noch nicht ausreichend

erprobte UHF-Technologie einzusetzen? Brauchen wir für unsere Arbeit, auch langfristig gedacht, überhaupt das Potenzial, das in der UHF-Technologie liegt? Wenn wir uns an unseren bibliothekarischen Vorentscheidern orientieren, wurde bereits 2007 festgestellt, dass damals nach Schätzungen einiger Experten und Marktplayer ca. 1 700 bis 1 800 Bibliotheken mit der Transpondertechnik ausgestattet waren und fast 450 Millionen Medien ein Smart Label trugen. Dabei war aber erstaunlich, dass nicht die seit Anfang des 21. Jahrhunderts ständig im Blickpunkt stehende UHF-Technologie dominierend ist, sondern in 90 % der Fälle die weltweit zugelassene HF-Frequenz mit 13,56 Megahertz. Diese kann mit dem ISO 15693 Standard überall und ohne Einschränkungen eingesetzt werden. Sind das nicht Kennzeichen für eine erprobte Technologie?

Wir wollen in der Logistik-Kette keine Bierfässer in Deutschland suchen oder den Weg des Käses von Spanien an die Verkaufstheke verfolgen und auch nicht den gegenwärtigen Standort von Schnittblumencontainern ermitteln. Das sind alles Anwendungen, die mit der UHF-Technologie möglich sind. Wir brauchen einen örtlich begrenzten Einsatz in einer Bibliothek, der unsere Bestände sichert und den Nutzerinnen und Nutzern die Arbeit erleichtert und Wartezeiten verkürzt. Immerhin reden wir über eine Investition von zunächst etwa einer halben Million Euro, die nicht auf das falsche, weil demnächst lahmende Pferd gesetzt werden soll, aber - um im Bild zu bleiben - auch nicht auf einen jungen Wildfang, der erst gezähmt werden muss. Was wir heute investieren, muss auch noch in zehn Jahren zweckgerecht funktionieren.

Was ich Ihnen geschildert habe, sind Eindrücke aus dem Leben eines altgedienten Bibliothekars, der in seiner nunmehr fast 40jährigen Dienstzeit vieles gesehen, vieles überlegt, aber auch nicht alles realisiert hat. Dabei waren die letzten 15 Jahre von einem technologischen Tempo begleitet, die einen hätten außer Atem kommen lassen, wenn man allen Trends hinterher gehechelt wäre. Sie haben sich zum Teil auch nicht als der Königsweg für unsere Arbeit, sondern als Holzweg erwiesen – ich denke hier nur an die Mikrofiche-Technologie im Benutzungsbereich.

Sie werden jetzt sicherlich die Gelegenheit nutzen wollen, sich mit Ihren Kolleginnen und Kollegen über die aktuellen Trends und Ihre Projekte auszutauschen. Suchen Sie nach den berühmten Vorbildern, auch neudeutsch best-practise genannt, um Ihre Einrichtungen fit für eine weiterhin ungewisse Zukunft zu machen.

Dazu wünsche Ihnen viel Erfolg.

RFID als Feld für politische Debatten und Überzeugungsarbeit

Lobbying, politische Kommunikation und Themenmanagement

Marco Althaus

Politische Aspekte der RFID-Technologie werden im Bibliothekswesen überwiegend sektorspezifisch diskutiert. In der Vertretung ihrer Interessen gegenüber politischen Entscheidungsträgern stehen bibliothekstypische Finanzierungs- und Organisationsfragen im Vordergrund. Dabei kann jedoch die sektorübergreifende Kenntnis des Lobbyings von Industrie und Handel hilfreich sein. RFID ist zudem wegen der Datenschutzproblematik gesellschaftlich sehr umstritten. Auch wenn die Proteste abgeebbt sind, sind kritische Organisationen nach wie vor politisch aktiv und begleiten die Einführung der Technologie. Daraus ergibt sich die Notwendigkeit, Umfeld, Stakeholder und Risiken kontinuierlich zu beobachten und sich auf Konflikte bei Gesetzgebung und staatlicher Regulierung der RFID-Technik einzustellen.

Einführung: Die Eskalation der RFID-Kontroversen

Auf dem Radarschirm der Politik ist Radiofrequenzidentifikation über Jahrzehnte ein unbedeutender Punkt gewesen, um dann plötzlich zum Auslöser intensiver Debatten zu werden. Das ist für High-Tech-Themen nicht untypisch. Die politische Reichweite von RFID vergrößerte sich gegen Ende der 1990er Jahre erheblich. Ausgelöst wurde dies durch die Verbreitung der Technik in verbrauchernahen Einsatzfeldern und die Entwicklung eines neuen Politikfelds.

Einerseits nahmen Regierungen und Gesetzgeber die Entwicklung der digitalen Zukunft und der »Informationsgesellschaft« strategisch und regulatorisch in den Blick. Andererseits erreichten RFID-Kritiker mit ihren Bedenken nun zahlreiche Bürger. Es kam zu öffentlichen Debatten und medienwirksamen Protesten, die die Politik zu Reaktionen zwangen. Zuerst in den USA, dann auch in Europa wurde RFID Gegenstand parlamentarischer Aktivitäten und Untersuchungen durch Aufsichts- und Regulierungsbehörden. Technikkritiker sowie Daten- und Verbraucherschützer spitzten die Debatten zu und organisierten sogar Boykottbewegungen. Eine wesentliche Rolle spielte dabei das Internet als Kommunikations- und Organisationsmedium für die rasch wachsende Szene vernetzter Initiativen im Feld Datenschutz, Informationsfreiheit, informationeller Selbstbestimmung und Bürgerrechte.

Zu Beginn der 2000er entwickelte sich die politische Debatte für die an der RFID-Einführung in Deutschland und Europa interessierten Unternehmen – insbesondere in Logistik, Handel und IT-Wirtschaft – zum Risiko: Sie beeinflusste die Anstrengungen,

Standards und ein rechtssicheres Rahmenwerk für RFID auf nationaler wie europäischer Ebene zu schaffen, öffentliche Fördermittel für Forschung und Entwicklung zu gewinnen und schließlich die Akzeptanz beim Verbraucher und Bürger zu sichern.

Der Staat war von Anfang an selbst betroffen. Im Feld der Sicherheitstechnologie ist der Staat ein wichtiger Kunde der IT-Wirtschaft, und er macht Vorgaben für Kunden des gesamten öffentlichen Sektors von Bundeswehr über öffentliche Kreditinstitute und Krankenkassen bis zu – natürlich – Bibliotheken und Archiven.

Eine scharfe, enge, RFID-spezifische Regelung wollten die Unternehmen nicht. Schon gar nicht sollte ein nationaler Alleingang Deutschlands erfolgen: Forderungen etwa nach der Aufnahme von RFDI ins Bundesdatenschutzgesetz und scharfen Strafen gegen Verstöße machten die Industrie nervös. Ein deutsches »Lex RFID« sollte aus Sicht der Industrie verhindert werden. Stattdessen sollte ein für die Unternehmen flexibler Empfehlungsrahmen (»soft law«) auf europäischer Ebene die Konfliktpunkte befrieden. Die deutsche Regierung sollte ihr Gewicht bei der EU für eine sanfte Lösung einsetzen.

Das sollte auch gelingen: Nach ersten Weichenstellungen 2006 (öffentliches Konsultationsverfahren zu RFID) beschloss die Europäische Kommission im Mai 2009 Empfehlungen zu Privatsphäre und Datenschutz bei RFID, die von den EU-Mitgliedstaaten in nationale Maßnahmen umsetzen müssen. Das Ergebnis war also eine flexible Regelung mit Spielraum für Interpretationen. Dabei kam es den RFID-Befürwortern zu Gute, dass die Kommission das »Internet der Dinge« vorrangig als positiven Teil ihrer »Digitalen Agenda«, der Lissabon-Strategie und des 7. EU-Forschungsrahmenprogramms verstanden wissen wollte. Die RFID-Entwicklung sollte zur Wettbewerbsfähigkeit Europas beitragen. Deshalb fielen die EU-Vorstöße zu Datenschutz, Informationspflichten und Sicherheit am Ende sehr maßvoll aus.

Das konnte 2003-2005 aber niemand absehen. Die politische Lage war äußerst problematisch, sowohl in der EU als auch in Deutschland. Mit großem Medienecho starteten Datenschutzorganisationen 2004 eine »Stopp RFID«-Kampagne gegen »Schnüffelchips« und den »gläsernen Verbraucher«. Sie brachten öffentlichen Zorn über die Kundenkarten- und »Future Store«-Projekte des Handelskonzerns Metro. 2005 verursachte der Streit um die Fußball-WM-Tickets politischen Wirbel. Besonders intensiv war die Publizität über RFID zwischen 2004 und 2007, wobei in der Publikumspresse Beiträge zu rechtlichen Aspekten, insbesondere Datenschutz, dominierten – 2004 gar bis zu zwei Dritteln der Presseartikel, wie der Zukunftsreport Ubiquitäres Computing für die Technikfolgenabschätzung des Bundestages feststellte (Deutscher Bundestag, 2010, S. 100). Die Firmen reagierten gereizt. Im August 2005 strahlte das ZDF-Magazin Frontal21 den Beitrag »Der gläserne Bürger – Überwachung per Funkchip« aus, gegen den Metro und der Fußballverband FIFA mit ihren Rechtsanwälten vorgingen. Das ZDF nahm das Video und das Sendemanuskript von der Website, jedoch kursierten beide kurze Zeit später wieder im Internet (LobbyControl, 2005).

Im Bundestag ließ die Opposition aus Grünen, FDP und Linken ab 2004 beim Thema RFID nicht mehr locker: Die Bundesregierung hatte sich mit parlamentarischen

Anfragen, Entschließungsanträgen, Ausschussberatungen und Plenardebatten zu RFID auseinanderzusetzen. In der 16. Wahlperiode ab 2005 zählt das Dokumentationssystem des Bundestags 102 parlamentarische Drucksachen und 24 Plenarprotokolle zu RFID von der Warenetikettierung bis zum biometrischen Reisepass (Deutscher Bundestag, 2011).

Die von den Bundesministerien für Wirtschaft und Verbraucherschutz ab Sommer 2004 initiierten Konsultationen »RFID und Verbraucherschutz« mit Handel, Industrie, Daten- und Verbraucherschützern hatten einen holprigen Start. Ein von der Standardisierungsorganisation GS1 Germany ausgearbeiteter Entwurf zur Selbstverpflichtung der Wirtschaft stieß auf Ablehnung der an den Konsultationen beteiligten Gruppen wie dem Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) und der Deutschen Vereinigung für Datenschutz (DVD), die den öffentlichen Druck durch ihre Kampagnen ständig erhöhten. Unternehmen sahen sich in der Defensive und genötigt, ihre RFID-Projekte zu rechtfertigen, teilweise zurückzufahren und Daten- und Verbraucherschützern entgegenzukommen (Hamann, 2006).

Das Informationsforum RFID – ein Kind der Berliner Republik

Die politische Kommunikation der RFID-Befürworter blieb zunächst unterentwickelt, langsam und fragmentiert. Eine Reihe von Spitzen-, Branchen-, Fach- und Berufsverbänden der Wirtschaft setzte sich für RFID ein: der Bundesverband der Deutschen Industrie (BDI), Bitkom für die IT-Wirtschaft, der Elektrotechnik-Verband VDE, der Handelsverband HDE, diverse Logistikverbände, die Gesellschaft für Informatik und andere, unterstützt und ergänzt durch punktuelle Interventionen der Unternehmen mit ihren spezifischen Belangen. Besonders effektiv schien das jedoch nicht.

In die Defensive geraten, warb der Metro-Konzern daher bei vielen Partnern um einen koordinierten, strategischen und themenspezifischen Ansatz. Resultat der Absprachen war im April 2005 die Gründung des Informationsforums RFID e.V. Das IF sollte eine Plattform sein, die den »Gefahren« der »falschen Einschätzungen« und des »großen Informationsdefizits« wehren und »das innovative und wirtschaftliche Potenzial der Technologie« in der öffentlichen Diskussion verdeutlichen sollte, so die Geschäftsführerin Andrea Huber (Stegherr, 2005b, S. 49). Die promovierte Juristin war zuvor Government Affairs Director bei Microsoft Deutschland und Leiterin der Abteilung Internationale Interessenvertretung der Deutschen Telekom. Sie baute das IF auf, dem für fünf Jahre eine Schlüsselrolle im Lobbying und der politischen Öffentlichkeitsarbeit zukommen sollte.

Modell Strategische Allianz

Das IF war weder Verband noch Ad-hoc-Koalition. Vielmehr handelte es sich um eine Organisationsform neuen Typs: eine Strategische Allianz mit eigener Infrastruktur und professioneller Geschäftsführung, engem Fokus und zeitlich befristetem Auftrag für die politische Kommunikation in Kampagnenform. Das IF wirkte als Projektagentur. Von vornherein war klar, dass das IF nur solange bestehen würde, bis die schwierige politische Lage gemeistert und die Weichen für die allgemeine Gesetzgebung gestellt waren.

Strategische Allianzen sind Kinder der Berliner Republik: Medienwirksame, schlank strukturierte, projektorientierte, flexible Interessenkoalitionen oft ungewöhnlicher Partner jenseits der etablierten Verbändestrukturen. Die Begrenzung auf ein Ziel oder wenige Themen erleichtert es, Interessengegensätze ungleicher Partner auszuklammern. »Lobby im Schnellboot« und »schnelle Eingreiftruppe der Unternehmen« nannte sie das Fachblatt *Politik & Kommunikation* (Stegherr, 2005a, S. 46).

RFID wurde zum Paradebeispiel für das Novum der Strategischen Allianzen. Andere Allianzen der ersten Jahre waren das Informationszentrum Mobilfunk (fokussiert auf gesundheitliche Ängste bei Mobilfunkantennen), die Allianz pro Schiene (die gegen Autobahn- und Flugverkehrausbau Bahninteressen vertritt, und zwar als gemeinsame Plattform von Bahnen, Bahnindustrie, Umwelt- und Fahrgastverbänden sowie Gewerkschaften), die »Existenzfrage Zucker« (mit der sich die Zuckerindustrie zur EU-Zuckerreform zu Wort meldete), die Intiative »Druck gegen Abgaben« (der Druckerhersteller bei der Urheberrechtsnovelle), die »Initiative Luftverkehr« oder »Mehr Bonus für Kunden« (von Handels- und Finanzfirmen gegen das Rabattgesetz). Jüngst kam »Die Lebensmittelwirtschaft« hinzu, eine Allianz von Industrie, Handel, Handwerk und Gewerkschaft NGG, die industriekritischen Vereinen wie Foodwatch die Stirn bieten soll.

Solche Allianzen sind für mehr als einen kurzfristigen Interessenabgleich gedacht, nämlich für eine gemeinsame Steuerung bei komplexen Vorhaben über mehrere Jahre hinweg (von Münchow, 2006, S. 39). Zudem steht die externe Kommunikation, nicht die Gremienarbeit oder Dienstleistungen für Mitglieder im Vordergrund: »Allianzen sind darauf ausgelegt, die Öffentlichkeit und somit die Politik für ihr Thema zu gewinnen. Sie arbeiten nicht ausschließlich im Verborgenen – sie wirken nach außen nicht nach innen. Dies unterscheidet sie grundlegend von einem Verband« (S. 40).

Geschäftsführerin Huber nannte das IF eine »Plattform für Diskussionen über Datenschutz, Verbraucherschutz und andere kritische Themen«. PR- und Politikverantwortliche der Mitglieder trafen sich alle zwei Monate im Arbeitskreis Kommunikation, um sich auszutauschen und zu koordinieren. Das Forum sollte »Scharnierfunktion« haben und Synergien erzeugen:

> »Als strategische Allianz spart man Ressourcen und bündelt Know-how, zum Beispiel für Flyer oder die Internetseite. Unternehmen wollen sich zudem gegenüber der öffentlichen Kritik nicht unbedingt einzeln positionen. Sie sind dankbar, wenn eine neutrale Plattform die Diskussion in ihrem Sinne führt. [...] Es gibt bei uns keine hauptamtlichen Funktionäre und keine gewachsene Kassenwartsmentalität, wie sie althergebrachte Verbände zum Teil auszeichnet. Bei uns geht es in erster Reihe ums Thema, für uns zählt der konkrete Erfolg« (Stegherr, 2005b, S. 49).

Die Netzwerkarbeit zwischen Allianz und den Mitgliedern kann als »Lobbying nach innen« bezeichnet werden, so Huber (2007, S. 9). Das Informationsforum RFID folgte auch dem Prinzip, möglichst ungewöhnliche Partner zu einigen. »Je bunter und je breiter eine Allianz aufgestellt ist, desto mehr potenzieller Erfolg steckt in ihr. Gerade diese Breite verleiht der Allianz das Attribut ›strategisch‹ «, betont von Münchow (2006, S. 40). In

der Tat: Das IF vereinte den IT-Verband Bitkom und die Bundesvereinigung Logistik, Logistiker wie DHL und Intermec, Industriekonzerne wie Volkswagen und Philips, Konsumgüterhersteller wie Procter & Gamble, Gillette und Henkel, IT-Unternehmen wie IBM, T-Systems, Oracle, Hewlett-Packard, NXP oder SAP und Siemens sowie den Einzelhandelskonzern MetroGroup.

Das war keine allzu große Gruppe. Vielleicht war das gut so, denn das Risiko des Scheiterns ist bei sehr großen Allianzen durch hohen Abstimmungsbedarf, Unterschiede in Struktur und Selbstverständnis der Partner, ungleiche Belastung und Konfliktmanagement ungleich höher, wie Wiebusch (2005, S. 219) anmerkt:

> »Dieser Koordinationsbedarf kann eine neue Organisation bei der Umsetzung ihrer Ziele deutlich verlangsamen, möglicherweise sogar lähmen und so die Hoffnungen auf große Schlagkraft enttäuschen.« (S. 219)

Während etwa die Allianz pro Schiene mehr als 50 Mitgliedsorganisationen (darunter viel Nonprofit-Gruppen) umfasst, blieb das IF stets auf rund ein Dutzend beschränkt, fast ausschließlich Großunternehmen. Ob man unter sich bleiben wollte oder die Neurekrutierung nicht gelang, ist unklar. In der Anfangszeit war z. B. mehrfach die Rede davon, die Luftverkehrsbranche einzubeziehen. Das materialisierte sich jedoch nicht. Auffällig ist zudem, dass die IT-Branche breit repräsentiert war, der Einzelhandel aber nicht. Weder war der Dachverband HDE Mitglied noch die großen deutschen Handelsgruppen wie Rewe, Edeka, Tengelmann, Otto, Arcandor oder die Discounter Aldi, Lidl, Netto oder Schlecker. Das IF suchte allerdings oftmals punktuell nach Partnern außerhalb seiner Mitgliedschaft: So wurden vom IF diverse Positionspapiere in die Politik eingespeist, die die Logos des Einzelhandelskonzerns GroupeCarrefour, des HDE, BDI, des Deutschen Industrie- und Handelskammertags (DIHK), des Automobilindustrieverbands VDA oder des Markenverbands trugen (Informationsforum RFID, 2011).

Bezeichnenderweise stellten die Mitglieder keinen Unternehmenslenker als Vorsitzenden an die Spitze des IF-Trägervereins, sondern den Geschäftsführer des Fraunhofer-Instituts für Materialfluss und Logistik und Professor der TU Dortmund, Michael ten Hompel. Außer ihm war allerdings am IF keine einzige akademische Einrichtung beteiligt. Mit dem Wissenschaftler als Frontmann und Sprecher wurde eine neutrale Expertenautorität des IF suggeriert.

Lobbying und begleitende öffentliche Kommunikation

Die Lobbyarbeit des IF umfasste das Kontaktmanagement mit Entscheidungsträgern, für die Hintergrundgespräche, Parlamentarische Abende, Fachveranstaltungen in Bund und Ländern und sonstige Events arrangiert wurden. Das IF trat mit seinen aus den Mitgliedsunternehmen rekrutierten Experten bei Ausschussanhörungen und bei Konsultationen auf, steuerte Positionspapiere, Rechts- und Fachgutachten sowie Studien und Umfragen bei. Das IF war nicht nur in Deutschland aktiv, sondern auch in Brüssel, wo es mit Schwesterorganisationen wie dem britischen RFID Centre oder der RFID Platform Nederland zusammenarbeitete. Der Öffentlichkeitsarbeit dienten mehrere Websites

für Politik, Journalisten, Wissenschaftler und Bürger. Das IF produzierte Broschüren, Berichte, Materialien für die Verbraucherkommunikation. Es organisierte Interviews, Pressegespräche sowie Messeauftritte (z. B. CeBIT) und Roadshows für mittelständische Unternehmen. Zum Teil ließ sich das personell schlanke IF (drei feste Mitarbeiter) von Public-Affairs-Agenturen wie Pleon und externen Pressebüros sowie den Stäben der Mitgliedsfirmen unterstützen.

Der erste Aufschlag fand an prominenter Adresse statt: im Leibniz-Saal der Berlin-Brandenburgischen Akademie der Wissenschaften, wo sich das IF Abgeordneten, Ministerialbeamten und Journalisten vorstellte. Der Auftakt erfolgte spät, erst ein halbes Jahr nach Eröffnung des IF-Büros. Das Timing geriet unter die Räder der großen Politik: »Ursprünglich wollten wir im Herbst 2005 richtig durchstarten. Das hat sich leider verzögert, weil sich die Koalitionsverhandlungen zwischen CDU und SPD sehr lange hingezogen haben«, berichtete Geschäftsführerin Huber später. »Es standen zu dieser Zeit einfach keine Sprecher aus der Politik zur Verfügung, sodass wir unsere Auftaktveranstaltung auf Januar 2006 verschieben mussten« (Informationsforum RFID, 2009d). Kritiker wurden dazu nicht eingeladen. Sie kamen trotzdem. »Mitglieder des FoeBuD standen im Januar 2006 tatsächlich mit Plakaten vor der Location unserer Auftaktveranstaltung«, wunderte sich Huber noch drei Jahre später (Informationsforum RFID, 2009d, S. 8).

Per Pressemitteilung attackierten FoeBuD und DVD »die unkonstruktive Haltung der RFID-Industrie, die lieber kritikfreie Jubelveranstaltungen durchführt statt sich konstruktiv am kritischen Dialog zu beteiligen.« Kritik solle mit einer PR-Offensive erstickt werden, während die Wirtschaft bei den Konsultationen der Bundesregierung »Hinhaltetaktik« betreibe. Sie wolle »nur Zeit gewinnen, um Fakten zu schaffen« (FoeBuD, 2006).

Die Kritiker lagen durchaus richtig. Zu jener Zeit waren viele RFID-Projekte noch weit von Serienreife und Marktdurchbruch entfernt. Die Arbeit des IF sollte eine zu frühe Verrechtlichung der Technologie verhindern. Dialogverweigerung kann man der IF nicht grundsätzlich vorwerfen. Allerdings suchte sich das IF sehr genau aus, mit wem es den öffentlichen Dialog führte. So nahmen IF-Vertreter eher auf Podien mit staatlichen Datenschutzbeauftragten oder Repräsentanten der Verbraucherzentralen Platz als mit FoeBuD und DVD. Das IF beobachte ihre Aktivitäten und nahm ihre Argumente auf. Zu keiner Zeit ließ sich das IF aber auf Schaukämpfe mit ihnen ein, deren Polarisierungsversuche zunehmend ins Leere liefen.

Einflussnahme durch Politikberatung und Kooperationsprojekte

Vorrang hatten die tatsächlichen Entscheidungsträger. Für sie wollte das IF konstruktiver Politikberater mit Expertenstatus und Partner sein, keine aggressiv fordernde, kritisierende oder jammernde Interessenvertretung. In zahlreichen Publikationen fällt auf, wie häufig das IF und das bei RFID federführende Bundesministerium für Wirtschaft und Technologie sich gegenseitige Wertschätzung ausdrückten. Der gute Zugang zu Fachreferaten und zur Hausleitung ermöglichte gemeinsame Projekte und Veranstaltungen. Als Deutschland 2007 die EU-Ratspräsidentschaft innehatte, gewährte das Ministerium bei der EU-High-Level-Konferenz »RFID: Towards the Internet of Things« dem IF eine

prominente Expertenrolle, die sich auch im Abschlussbericht »European Policy Outlook RFID« niederschlug – ein Arbeitspapier mit direktem Einfluss auf Brüssel (Bundesministerium für Wirtschaft und Technologie, 2007). Das Ministerium förderte eine von IF und dem Softwarehaus Oracle betreute bundesweite Veranstaltungsreihe für den Mittelstand (Informationsforum RFID, 2008a). Beide schrieben gemeinsam einen (vom IF verwalteten) RFID-Mittelstandspreis aus (Informationsforum RFID, 2009). Das Ministerium war Schirmherrn für den IF-Logo-Wettbewerb »RFID zeigt Gesicht!«, bei dem Designstudenten Entwürfe für eine Kennzeichnung von verbrauchernahen Anwendungen einreichten (Informationsforum RFID, 2008b) – eine Aktion, die der FoeBuD übrigens mit einem Gegenwettbewerb für ein Warnzeichen beantwortete (FoeBuD, 2008).

Ein kurzer Draht bestand auch zur EU-Kommission, die das IF in seine Stakeholder-Beratungsgruppe zu RFID einlud. Sie rief zur CeBIT 2009 eine auf drei Jahre angelegte Initiative »RFID in Europe« ins Leben, in die das IF als eine von 25 RFID-Institutionen aus 17 Staaten eintrat. Das IF wurde zum Gründungsmitglied des EU-finanzierten RACE-networkRFID (»Raising Awareness and Competitiveness in Europe«). Das IF übernahm ganz offiziell für die EU die Kommunikationsaufgabe, »Public Awareness« für RFID zu fördern, was das IF als Förderung der »Akzeptanz« übersetzte (Quack, 2009).

Bei so enger Kooperation ist nicht überraschend, dass jegliche öffentliche Kritik des IF an der Politik diplomatisch verpackt wurde. In Interviews und Pressemitteilungen verzichtete das IF auf harsche Wortwahl. So war es etwa bei der Branchenkritik an der Empfehlung der Kommission, Verbrauchern in jedem Fall eine Chip-Deaktivierung zu ermöglichen. Der Mitgliedsverband Bitkom äußerte sich oft prononcierter: Bei der CeBIT 2009 betonte das IF die positive Zusammenarbeit mit Brüssel, während Bitkom die Empfehlung als überflüssig bezeichnete und vor bürokratischen Hemmnissen warnte, die den Markt verunsicherten und Investitionen behinderten (Kümmerlen, 2009). So teilten sich die Akteure die Rollen.

Selbstverständlich lobbyierten und informierten die IF-Mitgliedsverbände und Mitgliedsunternehmen parallel eigenständig in Sachen RFID weiter, oftmals von Beratern, Agenturen und Anwaltskanzleien unterstützt. Die dabei eingesetzten Ressourcen sind nur punktuell bekannt geworden, beispielsweise im Sponsoring: Das Bundesministerium für Wirtschaft und Technologie ließ sich 2007 die EU-High-Level-Konferenz »RFID: Towards the Internet of Things« u.a. von Metro (30.000 Euro), IBM (30.000 Euro), dem mit IF en kooperierenden IT-Verband AIM (10.000 Euro) und dem Softwarekonzern SAP (15.000 Euro) sponsern (Bundesministerium des Innern, 2009). Die Agentur Pleon, die sowohl für das IF als auch die Metro Group arbeitete, trat mit 30.000 Euro als Kofinanzier eines Seminars für Lokaljournalisten der Bundeszentrale für politische Bildung auf, Thema »Intelligenz im Supermarkt – mit dem Einkaufswagen in die Zukunft« (Denkler, 2007).

Politische Bilanz und vorläufiges Ende

Trotz vieler Anfeindungen hat das IF fraglos viele Ziele erreichen können. Dazu gehört die Beruhigung und Normalisierung der öffentlichen Debatte, aber explizit auch, was

regulatorisch *nicht* geschah: Kein deutsches Gesetz wurde auf den Weg gebracht, keines geändert. Die Bundesregierung entschied, es gebe keinen Bedarf (Deutscher Bundestag, 2008).

Auch auf EU-Ebene kam es zu keinem Rechtsakt. Statt Parlament und Rat eine Richtlinie mit Gesetzeskraft vorzuschlagen, beließ es die Kommission im Mai 2009 bei einer Empfehlung für die Mitgliedstaaten (Europäische Kommission, 2009a). Das wurde im »Aktionsplan für Europa« zum »Internet der Dinge« vom Juni 2009 bestärkt (Europäische Kommission, 2009b). Das Europäische Parlament hingegen forderte im Juni 2010 konsequentere Datenschutzdurchsetzung und gab der Kommission den Auftrag, einen klaren Rechtsrahmen auszuarbeiten. Es sei absehbar, dass die von der Kommission bevorzugte Selbstregulierung der Wirtschaft nicht die gewünschten Ergebnisse bringen werde (Europäisches Parlament, 2010). Es ist offen, ob und wie die Kommission dem künftig folgt. Sie wartet erst einmal die nationalen Umsetzungsberichte ab. Die EU-Empfehlungen sind nach heutigem Stand sehr liberal und kein regulatorisches Risiko. Das mag sich künftig ändern, doch bis dahin dürfte die RFID-Technologie fest im Alltag verankert sein.

In der Gesamtsicht dürften die Träger des IF mit der fünfjährigen Leistung zufrieden sein. Festzuhalten ist, dass das Erfolgsgeheimnis nicht allein beim kleinen IF-Büro lag, sondern im Multi-Voice-Lobbying, bei dem die Mitglieder ihre jeweiligen Kanäle selbstständig nutzten. Das IF war eher Clearingstelle als Kommandozentrale.

2010 endete die Tätigkeit des IF in Berlin. Die Berliner Geschäftsstelle und der Trägerverein wurden aufgelöst, Huber wechselte zum Verband Deutscher Kabelnetzbetreiber, das IF als »Marke« kam unter das Dach von GS1 Germany in Köln – weitab der politischen Schaltstellen. In Köln geht es nun um technische Details und Beratung der RFID-Anwender bei der Umsetzung der EU-Empfehlungen. Schon im IF-Jahresbericht 2009 deutete Huber an:

> »Die beste Entwicklung – auch für unsere Mitglieder – wäre eigentlich, dass man uns gar nicht mehr braucht. Wenn wir irgendwann alle kritischen Fragen lösen können und RFID in der Politik und bei den Verbrauchern akzeptiert ist, hat sich unser Zweck erfüllt« (Informationsforum RFID, 2009c, S. 11).

Die tatsächliche Auflösung anderthalb Jahre später mag man als Indiz deuten, dass der Auftrag erfüllt war. Ganz verschwinden sollte das IF nicht. »Die Markenbekanntheit hat für uns eine große Bedeutung. Daher wird das RFID-Informationsforum nach außen hin seine Visibilität weiterhin behalten, nur organisatorisch sind die Stakeholder breiter aufgestellt«, erläuterte der GS1-Geschäftsführer Jörg Pretzel im Fachmagazin *RFID im Blick*. GS1 habe eine »viel breitere Unternehmens- und Branchenbasis«. Der neue Schwerpunkt: »Wir wollen das Thema Verbraucher- und Datenschutz enger an die operativen Umsetzungsthemen heranführen, wobei wir dieses auf einer größeren Basis behandeln« (RFID im Blick, 2011).

Lobby-Lektionen

Was lässt sich aus dem Interessenvertretungsmodell des Informationsforums RFID lernen, insbesondere für Bibliotheken? Zum einen fällt die konsequent kooperativ-konstruktive Haltung auf, die in der seinerzeit äußerst kritischen Lage ja nicht selbstverständlich war. Das IF mied jeglichen polarisierenden Streit, jeden scharfen Angriff, aber auch jedes Jammern wie der Teufel das Weihwasser. Das erfordert hohe Kommunikationsdisziplin und ist mehr als nur eine Stilfrage. Das IF blieb stets bei seinen Kernbotschaften, was durch die zwar nicht homogene, aber recht kleine Mitgliedergruppe erleichtert wurde.

Klare Adressatenorientierung durchzog sämtliche Aktivitäten. Für alle Zielgruppen (Politiker, Beamte, Journalisten, Verbraucher) gab es geeignete Dialogangebote. Das IF suchte die Kongruenz mit der Themen-Agenda der Politik. Es bot sich als Partner, Berater und Dienstleister an, um die Ziele der Politiker und Behörden erreichen zu helfen und diese in einem guten Licht dastehen zu lassen. Das IF beanspruchte Meinungsführerschaft beim RFID-Thema. Dennoch ließ es sich gern in die Aktivitäten politischer Partner einbinden und band sie ein. Das IF setzte sogar im offiziellen Auftrag und mit finanzieller Förderung des Wirtschaftsministeriums und der EU-Kommission Kommunikationsprojekte um. Es wurde zum ausführenden Organ der Politik.

Die ständige Suche nach Projekt- und Kooperationspartnern sowie Vernetzung und behutsamer Koordination war ein erkennbares Markenzeichen des IF. Dieser Outreach-Ansatz vergrößerte die Reichweite und signalisierte der Politik, dass das IF zahlreiche informell Verbündete hatte. Das IF vertrat Konzern- und Brancheninteressen, aber argumentierte sektorübergreifend mit dem Nutzen für andere, für Mittelstand, Verbraucher, Gemeinwesen, Wirtschafts- und Technologiestandort.

Ein Mehrwert ergab sich auch aus der internationalen Orientierung: Das IF vermittelte zwischen Berlin und Brüssel sowie zwischen EU-Mitgliedsländern. Vernetzt mit ähnlichen RFID-Plattformen in Europa, beteiligte es sich an der europäischen Debatte und war quasi die offizielle Vertretung und Stimme der deutschen RFID-Anwender. Diese Stellung im Ausland hatte Rückwirkung auf den Einfluss im Inland.

Der Großteil der Arbeit kann transparent genannt werden: Wer hinter dem IF stand und welche Interessen verfolgt wurden, war kein Geheimnis. Als fragwürdig erscheint höchstens die Berufung eines Wissenschaftlers als Vorsitzenden eines Vereins, der mit Wissenschaft wenig zu tun hatte. Substanziell konnten allerdings auch hyperkritische Watchdog-Gruppen wie z. B. LobbyControl dem IF keine Vorwürfe über unsaubere Arbeit machen.

RFID-Lobbying bei Bibliotheken

Verglichen mit den Ressourcen internationaler Konzerne muss das RFID-Lobbying bei Bibliotheken kleine Brötchen backen, keine Frage. Auch strukturell und inhaltlich sind Unterschiede festzustellen: Beim Fokus und den Zielen, bei den politischen

Entscheidern, den Argumenten und den Instrumenten. Das IF-Modell ist keine perfekte Blaupause. So wird Bibliotheken eher als den IF-Mitgliedern Legitimität als Träger öffentlicher Interessen zugestanden, was Möglichkeiten einer härteren kommunikativen Gangart einschließt. Bibliotheken haben durch ihre Nutzer eine viel breitere Basis, die sich mobilisieren ließe. Das IF versuchte das Vertrauen der Verbraucher durch Informationskampagnen zu gewinnen, für RFID mobilisieren wollte sie sie nicht. Bibliotheken könnten hier theoretisch anders vorgehen – wer Bürger für die auskömmliche Finanzierung der Bibliotheken mobilisiert, könnte auch die Modernisierung der Technik einschließen.

Andererseits ist das IF ein Vorbild, wie sich eine Interessengruppe ein Profil als gefragte Experten geben kann, die die Agenda der Politik unterstützen, statt sie zu kritisieren. Anpassung der Strategie an Bedürfnisse der Entscheidungsträger, Lobbying als Politikberatung, Einflussnahme durch Kooperationsprojekte, Vernetzung und Dienstleistung sind hier die Stichworte.

Lobbying unter Haushaltszwang

Zwar zielte die Wirtschaft auch auf staatliche Subventionen für die RFID-Forschung und Verbreitung ab, doch stand bei ihrer Lobbyarbeit der rechtliche Rahmen im Vordergrund. Bibliotheken haben dagegen bei ihrer Beschaffung vorrangig ein finanzielles Problem. Sie müssen die öffentlichen Haushälter in Ländern und Kommunen überzeugen. Das ist ein völlig anderer Adressatenkreis. Nur wenige dieser Politiker verfolgen intensiv und fachkundig die rasante Entwicklung der Informationstechnik oder speziell der Bibliotheksinfrastruktur im digitalen Zeitalter. Pauschal gesagt, sind Politiker nicht in der Lage, von sich aus Aufwendungen für die technische Ausstattung von Bibliotheken zu begründen und zu rechtfertigen. Das steht bisweilen in umgekehrt proportionalem Verhältnis zur Selbsteinschätzung. Andere Interessengruppen haben es zudem von vornherein leichter, freundliche Akzeptanz für Investitionen komplexe Technik zu finden: wenn Meldeämter leistungsfähige Computer brauchen, Forscher und Gesundheitseinrichtungen Laborgeräte oder Feuerwehren Einsatzsimulatoren und Spezialgerät.

Investitionen in RFID kosten viele Steuermittel. An RFID in Bibliotheken ist aber per se politisch nichts Interessantes, es ist ein Spezialwunsch unter vielen, mit dessen Erfüllung Politiker nicht zum Helden der Nachbarschaft werden. Politiker haben in Zeiten klammer Kassen ohnehin Verteilungskonflikte zu bewältigen, die für die Wiederwahl kritisch sein können. So dürften sich die skeptische Argumente zugespitzt so zusammenfassen lassen: »Das ist purer Luxus«, »Für das Geld könnte man auch viele Bücher kaufen«, »Das versteht bei mir im Wahlkreis keiner«, »Meine Kinder wollen auch immer neues Computerspielzeug«, »Wenn wir das bewilligen, müssen wir beim Hallenbad sparen« oder, ganz egoistisch, »Bis sich das rentiert, bin ich in Rente.«

Ohnehin sind Bibliotheken stark von der Haushaltskonsolidierung betroffen. Viele stehen unter Haushaltssperren, von ihnen werden Etatkürzungen oder Gebührenerhöhungen verlangt. Erwerbungsetats sinken, Öffnungszeiten und Veranstaltungen werden reduziert und Bauprojekte gestrichen, Personalstellen bleiben unbesetzt oder geraten

unter den Rotstift, und manchmal droht die Schließung. Von einer »Aushöhlung« dieser Bildungsinfrastruktur zu sprechen, ist sicher nicht übertrieben (Deutscher Bibliotheksverband, 2010).

Das ist also kein freundliches Umfeld, um für teure Technik-Investitionen nebst hohen Folgekosten zu werben. Die allgemeine Situation ist nicht neu, weshalb Bibliotheken und ihre Verbände sich immer stärker der Lobby- und Medienarbeit zuwenden. Sie suchen international nach Vorbildern und tauschen sich über Best-Practice-Beispiele aus, wie auch an einer wachsenden Zahl von Lobby-Handreichungen der Verbände sowie Ratgebern und Handbüchern speziell für Bibliotheken abzulesen ist. Vorerst bleibt die Beobachtung richtig, dass Bibliotheken selbst in bildungs- und innovationspolitischen Debatten Zaungäste sind, nur punktuell PR-Erfolge verzeichnen, Defizite bei der Vernetzung aufweisen und strategisch, taktisch und operativ »nur ansatzweise das Niveau einer Pressure-Group« erreichen (Ratzek, 2010, S. 33). Andere Interessengruppen kontern das Politiker-Argument, die Kassen seien leer, mit höherem politischem Druck, auf den die Politiker dann reagieren müssen. Das fällt Bibliotheken schwer.

Vier Argumentationslinien für die RFID-Beschaffung

Druck auszuüben, ist allerdings nicht der einzige Weg. Es geht durchaus um inhaltliche Argumente: solche, die den Nutzen für den Politiker und seine Agenda sowie nicht bibliotheks-, kultur- und bildungsspezifische Ziele betonen. Wie im Lobbymodell des IF geht es um die Kongruenz eigener und Politikerinteressen. Statt über eigene Probleme zu sprechen, spricht man über die Gemeinsamkeiten der Agenda – und präsentiert Lösungen.

Hier lohnt sich der Blick auf internationale Erfahrungen. Der US-Bibliothekenverband ALA beispielsweise hat in seiner »Advocacy University« ein umfassendes Argumentationspaket geschnürt, wie man auch in Zeiten eine Wirtschaftskrise Wert und Rendite von Bibliotheksinvestitionen gegenüber Politik und Medien vermittelt: Das »Advocating in a Tough Economy Toolkit« ist ein Werkzeugkasten mit Sprechzetteln, Fallbeispielen, Checklisten und Hinweisen für den Dialog mit Politikern, Behördenchefs und Journalisten. Auch wie man Bürger mobilisiert und mit anderen Organisationen Bündnisse aufbauen kann, wird erläutert (American Library Association, 2011).

Darauf aufbauend könnte man die zentralen politischen Argumente für RFID-Beschaffungsinvestitionen in vier Komplexe zusammenfassen: das Kundenservice-Argument, das fiskalische Argument, das wirtschaftspolitische Argument und das High-Tech-Argument.

Das Kundenservice-Argument

RFID ist ein Beitrag zu höherer Leistungsfähigkeit im Dienst am Kunden – durch Schnelligkeit, Bedienungsfreundlichkeit und Reduzierung von Fehlern. Dass Verwaltungen und öffentliche Betriebe bürgernah, im Sinne von Dienstleistung kundennah und nutzerorientiert sein sollen, hat hohe Priorität bei Politikern und Verwaltungsleitern. Die

Ansprüche der Bürger sind gewachsen. Das seit den 1990ern populäre »Neue Steuerungsmodell« (NSM oder New Public Management) kennt Leistungskennziffern, Benchmarkings, Produktkataloge, Outputs, Qualitätsmanagement. Auch wenn der Stern des NSM gesunken ist: Bürgermeister, Landräte, Minister sind stolz, wenn sie die unternehmerische Leistungsfähigkeit ihrer Einrichtungen bilanzieren können.

Das fiskalische Argument

RFID spart bares Geld – die Wirtschaft setzt auf RFID und weiß, was sie tut, wenn sie hier massiv investiert. Sie will Kosten sparen, Abläufe optimieren, die Wirtschaftlichkeit, Leistungs- und Wettbewerbsfähigkeit verbessern. Es geht um Rationalisierungseffekte.

Was für die Wirtschaft richtig ist, kann für Bibliotheken und öffentliche Haushalte nicht falsch sein: RFID liefert höhere Effizienz der Dienstleistungen und eine bezifferbare Rendite der durch Investitionen verbesserten unternehmerischen Tätigkeit.

Nun sind Politiker gegenüber den Amortisierungsversprechen bei IT-Investitionen inzwischen skeptisch geworden. Aus gutem Grund und schlechten Erfahrungen heraus: Hard- und Softwareanschaffungen werden ständig von der technischen Entwicklung überholt, was bei den komplexen IT-Systemen dezentralisierter öffentlicher Verwaltungen besonders problematisch ist und teuer wird. Das ist auch bei Bibliotheks-IT nicht abzustreiten. Gleichwohl können Bibliotheken bei RFID auf eine lange Nutzungsdauer verweisen, und ihre Systeme sind kleiner als in der allgemeinen Verwaltung.

Es wäre aber falsch, das fiskalische Argument nur auf den IT-Betrieb zu beziehen. Vielmehr geht es um den fiskalischen Wert der Bibliotheken für die Ziele, die Staat und Kommunen in Wirtschafts-, Arbeitsmarkt-, Sozial-, Bildungs- und Standortpolitik mit anderen Haushaltsausgaben erreichen wollen. Bibliotheken sind wirtschaftliche, effektive Dienste, die diese Ziele erreichen helfen. Eine Investition in RFID erhöht diesen Beitrag zur besseren Ausnutzung begrenzter Haushaltsmittel. Auch das kann man vorrechnen.

Interessant ist RFID auch deshalb, weil dafür z.T. Fördermittel der EU bereitstehen. Zwar ist eine Kofinanzierung mit eigenen Haushaltsmitteln notwendig, die Hebelwirkung ist jedoch dank der EU-Gelder ungleich größer.

Ein weiteres fiskalisches Argument ist das, welches Personalvertretungen und Gewerkschaften naturgemäß nicht gerne hören, Haushaltspolitiker aber schon: RFID hat Effekte auf die Personalbewirtschaftung. Einsparung und Umwidmung von Stellen und Aufgaben ist möglich. RFID ist pauschal kein Arbeitsplatzvernichter, aber sehr wohl ein Rationalisierungsinstrument. RIFD sichert qualifizierte Arbeitsplätze, macht aber Routineaufgaben entbehrlich. Eine Bibliothek, die Personaleinsparungen erbringen muss, hat hier ein gutes Argument in der Tasche: Wenn wir mit weniger Mitarbeitern mehr leisten müssen, dann bitte mit einer Technik, die uns das ermöglicht.

Das wirtschaftspolitische Argument

RFID heißt Wirtschaftsförderung. Die Anwendung und Beschaffung von RFID kann die regionale Wirtschaft stärken. Projekte der öffentlichen Hand zur Einführung neuer Technologien demonstrieren die Marktfähigkeit von Anwendungen und lösen so private Investitionen aus. Bibliotheken haben eine sichtbare Vorbild- und Vorreiterfunktion. Die öffentlichen Hände haben durch ihre Beschaffungs- und Dienstleistungsaufträge bei der RFID-Einführung und Systemwartung zudem einen direkten Effekt auf die Auftrags- und Ertragslage sowie die Wettbewerbsfähigkeit privater Unternehmen. Haushaltsmittel für RFID-Investitionen fließen in die Kassen des örtlichen Mittelstands, der sich in der Anwendung wertvolle Erfahrungen und Know-how für den Markt sichert, auf dem RFID eine wachsende Rolle spielt – in Handel, Logistik und Industrie.

Weiter vergrößern Bibliotheken allgemein das Humankapital, indem sie Arbeitnehmern und Arbeitssuchenden sowie Menschen in Ausbildung helfen, ihre Beschäftigungsfähigkeit zu sichern und auszubauen. Durch RFID verbesserte Bibliotheksdienstleistungen vergrößern diese Möglichkeiten.

Diese Multiplikatoreffekte sollte man nicht unerwähnt lassen. Ganz besonders, wenn die Region sich einen Wachstums- und Innovationsplan gegeben hat oder sich an einem Wirtschaftsfördercluster beteiligt.

Das High-Tech-Argument

Ans wirtschaftspolitische Argument schließt sich das technologiepolitische an: Öffentliche Pilotprojekte haben Signal- und manchmal Leuchtturmwirkung für Technologien. RFID-Ausrüstung ist eine strategische Frage des Technologiestandorts, die der Träger der Bibliothek nicht unbeantwortet lassen kann. Nur Bibliotheken mit ausgebauten digitalen Dienstleistungen haben eine Zukunft. RFID ist unverzichtbares Element dieser Infrastruktur. Einrichtungen ohne RFID würden den Anschluss ans moderne Bibliothekswesen verlieren, sich abkoppeln und isolieren. Mit Luxusspielzeug hat das nichts zu tun: Ein zentraler Informationsdienstleister des 21. Jahrhunderts kann nicht mit den Technologien des 20. Jahrhunderts arbeiten. So wie der Nutzer heute in Bibliotheken Datenbanken und digitale Medien findet und nicht nur Bücher, so wie er elektronische und keine Zettelkataloge verwendet, so ist das Herz einer Bibliothek heute die IT im Hintergrund.

Überdies bietet die RFDI-Einführung der Bibliothek interessante Projekte von hoher Komplexität für die angewandte Forschung – ein Thema für die örtliche Universität, Fachhochschule oder Technikinstitute, die damit in der Wissenschaft oder einem Forschungscluster punkten können.

Diese politischen Argumente grenzen sich von den klassischen Argumentationslinien der Bibliotheksfinanzierung ab: Hier ist nicht oder nur indirekt die Rede von Kulturgütern, allgemeiner Bildungsbeteiligung und Chancengleichheit, dem Recht auf Informationszugang, sozialer Inklusion, von der Rolle als Begegnungs- und Kommunikationsstätte oder pädagogischen Aufgaben. So wichtig diese Argumente allgemein auch sind: Gerade

bei Technikinvestitionen wie RFID gerät man mit »weichen« Begründungen in eine rhetorische Sackgasse. RFID-Chips erfüllen keine kulturellen, sozialen oder pädagogischen Funktionen. Sie ermöglichen es höchstens durch Effizienzgewinne, dass sich Mitarbeiter mehr auf diese konzentrieren können.

Themenmanagement und kritisches gesellschaftliches Umfeld

Instruktiv ist die Arbeit des Informationsforums RFID für den sensiblen Umgang mit den *issues*, jenen kritischen, konflikthaften Themenfeldern, die externe Akteure – Anspruchsgruppen oder Stakeholder genannt – mitgestalten und bewusst eskalieren können.

Das strategische Kernproblem liegt darin, die Konfliktfelder und die einflussreichen Akteure rechtzeitig zu erkennen. Das ist die Aufgabe eines Frühwarnsystems oder der strategischen Frühaufklärung. Damit beschäftigt sich seit den 1970ern die Disziplin des Issues Management, ein Teilgebiet der Strategischen Managementlehre und der Risikokommunikation. Auf kontinuierliche Umfeld-Beobachtung soll danach viel Wert gelegt werden.

Zentral ist dabei die Problematik der »schwachen Signale«. Signale für Werte- und Erwartungswandel bei Stakeholdern und künftige Konflikte sind zu Anfang so schwach, dass sie oft übersehen werden. Erkennt man sie aber, hat man eine Chance, mit großem Spielraum frühzeitig in den Thematisierungsprozess einzugreifen, solange Deutungsmuster in Politik und Öffentlichkeit noch nicht festgelegt sind. Das Fenster schließt sich und schränkt die Handlungsmöglichkeiten ein, je mehr Akteure und Medien in die Thematisierung einsteigen (Rawe & Schulz, 2005, S. 13).

Handel und Industrie übersahen die »schwachen Signale« und gerieten in die Defensive. Bibliotheken sollten den Fehler nicht wiederholen. Konkret geht es um das Vertrauen in die RFID-Technologie und ihre Akzeptanz. Dieselben Akteure, die Handel und Industrie relevant waren, sind grundsätzlich auch Stakeholder RFID-nutzender Bibliotheken. Dieselben Befürchtungen und Zweifel, die die Einstellung zu RFID in Wirtschaft und Behörden prägen, sind für Bibliotheken relevant – auch wenn der spezifische Zuschnitt anders ist.

Bibliotheken sind gut beraten, dieses Umfeld mit seinen *issues* und Akteuren zu beobachten und zu analysieren. Immerhin ist der RFID-Einsatz in Bibliotheken mit den Funktionen für kommerzielle Lagerverwaltung und Inventur, im kundennahen Bereich aber auch mit Abrechnung, Kundenkarten und Diebstahlprävention der Einzelhandelsunternehmen vergleichbar – also genau jenen Einsatzgebieten, die für politische Kontroversen gesorgt haben. Ob und wie Konfliktthemen aktiv gesteuert werden müssen oder ein Dialog mit den Akteuren begonnen werden muss, ist eine Einzelfall-Entscheidung. Immun gegen Konflikte sind Bibliotheken jedenfalls nicht, so sehr sie auch beteuern, ein datensparsames, sicheres RFID-Modell zu betreiben.

Beim Einzelhandel lag das Datenschutzproblem auf der Hand, weniger wegen der Warenlogistik als vielmehr wegen der marketingrelevanten Verknüpfung mit Kundendaten über Einkaufsverhalten und persönliche Profile. Hier haben die Befürchtungen der Bürger, trotz mancher Übertreibungen, durchaus eine reale Basis. Ebenso plausibel sind die Probleme in der Sicherheitstechnik und Überwachung.

RFID-Befürworter kämpften mit dem Gespenst der »totalen Kontrolle«, das im vergangenen Jahrzehnt in Deutschland Zehntausende zu Protestaktionen und Demonstrationen (»Freiheit statt Angst«) auf die Straße brachte. Diese Mobilisierung belegt die Fähigkeiten von Interessengruppen wie FoeBuD oder Deutscher Vereinigung für Datenschutz (DVD), die seit Jahren Begriffe wie »Schnüffelchips« prägen. Sie arbeiten mit einer Koalition anderer Gruppen zusammen, so dem Chaos Computer Club (CCC), dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), dem Förderverein Informationstechnik und Gesellschaft (Fitug), der Humanistischen Union und der Internationalen Liga für Menschenrechte.

Das Spektrum reicht also von Netzaktivisten bis zu Bürgerrechtlern. Sie besetzen Nischen im Verbändewesen und sind keine Massenorganisationen. Gleichwohl ist ihr Einfluss nicht zu unterschätzen. So hat der Deutsche Bundestag den FoeBuD-Vorsitzenden und die Sprecherin des CCC 2010 als Sachverständige in die Enquete-Kommission Internet und digitale Gesellschaft (die auch eine Projektgruppe Datenschutz und Persönlichkeitsschutz umfasst) berufen, wo sie gleichberechtigt mit Bundestagsabgeordneten und anderen Sachverständigen, etwa ranghohen Wirtschaftsvertretern und Professoren, arbeiten. In der Enquete, die für eine Wahlperiode arbeitet, sind als Sachverständige weitere Vertreter von Organisationen zu finden, die bei der RFID-Debatte eine relevante Rolle gespielt haben, so die Gewerkschaft Ver.di oder der Verbraucherzentrale Bundesverband.

Wesentlich für den Einfluss von Nichtregierungsorganisationen ist es, die öffentliche Agenda über die Medien beeinflussen zu können. Ein Beispiel für Medienerfolge sind die »Big Brother Awards« des FoeBuD und seiner Bündnispartner, die sie als »Oscars für die Datenkraken« bezeichnen. Sie gingen mehrfach an RFID-Anwender: an den Metro-Konzern für seinen »Future Store« (2003), an den Deutschen Fußball-Bund wegen der WM-Tickets (2006), an die Deutsche Bahn wegen der BahnCard 100 (2008), an die Modemarke Peuterey und ihren Vertriebspartner Torsten Müller (2011), weil sie Kleidung mit verdeckt integriertem RFID-Chip in Verkehr brächten, der berührungslos auslesbar sei, ohne dass die Kunden das bemerkten (FoeBuD, 2011). FoeBuD & Co suchen weiter nach aktuellen Fällen. Es ist nicht ausgeschlossen, dass ein »Big Brother Award« demnächst Bibliotheken trifft – was sicher ein großes unangenehmes Medienecho mit sich brächte.

Das Nischenthema RFID erhält trotz seiner technischen Komplexität Aufmerksamkeit durch einen sensiblen rechtspolitischen Kontext und mediale Symbolik. Datenschutz und informationelle Bürgerrechte haben breite öffentliche Debatten ausgelöst, von Google Street View bis zu Datenlecks bei Facebook oder dem Apple iPhone, von der Mitarbeiterüberwachung bei Lidl, Deutscher Bahn und Deutscher Telekom bis zur

EasyCash-Affäre bei EC-Karten, von der Arbeitnehmerdatenbank Elena bis zur elektronischen Krankenakte und zu biometrischen Ausweisen. Dazu gehören ebenso Internetsperren, Vorratsdatenspeicherung, Videoüberwachung, Polizeirechte und Maßnahmen gegen Kriminalität und Terrorismus.

Die Novellierung des Bundesdatenschutzgesetzes 2009 erhielt entsprechend viel Aufmerksamkeit. Weitere Novellen sind wahrscheinlich, nicht zuletzt auf Druck der EU. Wahrscheinlich ist zudem eine Neustrukturierung der Datenschutzstellen, da der Europäische Gerichtshof (2010) in einem Vertragsverletzungsverfahren gegen Deutschland eine zu geringe Staatsferne moniert hat. Größere Unabhängigkeit der Datenschutzbeauftragten hätte wohl mehr politischen Aktivismus zur Folge – denkbar auch bei RFID.

Diese Debatten sind inzwischen in alle Bundestagsparteien eingedrungen. Zudem haben sie der 2006 gegründeten Piratenpartei einen hohen Mitgliederzuwachs und erhebliches Medieninteresse beschert und schließlich eine Reihe von Wahlerfolgen.

Es sei daran erinnert, dass es den RFID-Kritikern früh gelang, ihre Anliegen in den parlamentarischen Raum zu bringen – in den Bundestag über die Oppositionsfraktionen FDP, Grüne und Linke, aber auch ins Europäische Parlament und in die deutschen Landtage. Auf dieser Bühne erhalten die Themen Medienaufmerksamkeit und Beachtung der politischen Eliten.

Regierungsmehrheiten können Entscheidungen zwar abblocken, nicht aber die Themenwahrnehmung. Umgekehrt können Regierungen die Thematik von sich aus aufgreifen, auch in den Ländern. Gesetzgeberisch ist der Einfluss der Länder begrenzt, im politischen Agenda-Setting jedoch größer. Zudem können sie auf Landes- und Kommunalebene Regeln für den Einsatz im öffentlichen Sektor schaffen.

Kritik an und im Bibliothekswesen

Ein Beispiel für landespolitische Aktivitäten ist die Initiative der rheinland-pfälzischen Verbraucherministerin Margit Conrad vom Herbst 2010, die mit dem Landesdatenschutzbeauftragten einen »Verbraucherdialog« zu RFID mit Wirtschafts-, Berufs- und Verbraucherverbänden sowie Behörden ins Leben rief. Sie betonte die Notwendigkeit zur Regulierung von RFID, falls Selbstverpflichtungen der Wirtschaft nicht griffen. RFID sei ohne Transparenz nicht kontrollierbar, wirksame Kontrollen und Sanktionen seien nötig. Ein besonderer Fokus des Daten- und Verbraucherschutzes müsse der Einsatz im öffentlichen Sektor sein, beispielsweise in Bibliotheken (MUFV, 2010). Bemerkenswert ist, dass die von der Ministerin präsentierte RFID-Informationsbroschüre gleich auf zwei Seiten auf Bibliotheken zu sprechen kommt und als »Nachteile« des RFID-Einsatzes benennt: »Bei RFID-Einsatz im Bibliotheks- bzw. Büchereiausweis besteht bei spezieller Ausrüstung der Bibliotheken die Möglichkeit Bewegungsprofile zu erstellen«; »Bei Medienrückgabe allein mittels RFID erfolgt in der Regel keine Kontrolle des Mediums auf Beschädigung« sowie »Stellenabbau durch Automatisierung« (MUFV & Landesbeauftragterfür den Datenschutz, 2010). Wohlgemerkt, dies ist eine offizielle Regierungspublikation.

Bei den deutschen Nichtregierungsorganisationen ist festzustellen, dass Bibliotheken bisher kein prioritäres Zielobjekt gewesen sind. Strategisch betrachtet sind Konzerne und Sicherheitsbehörden ein dankbareres Ziel, wenn man Protest- und Medienwirkung sowie Mobilisierungspotenzial einrechnet. Dennoch steht RFID in Bibliotheken unter Beobachtung, beispielsweise beim FoeBuD. Der Verein äußerte sich bereits 2006 in seinem Grundlagenpapier »Unsere Positionen« beunruhigt über die Folgen der Standardisierung von Buchetiketten und Outsourcing von RFID-nahen Dienstleistungen bei Lieferanten sowie mangelnder Transparenz selbst geschlossener Systeme:

> »Ein Beispiel für den schon stattfindenden Einsatz von RFID in geschlossenen Systemen ist die Nutzung in Bibliotheken. ›Die Früchte des Zorns‹ in Bibliothek X hat einen anderen Code als derselbe Titel in Bibliothek Y. Obwohl RFID-Applikationen heute auf geschlossene Systeme beschränkt sind, wird es große Nachfrage nach standardisierter Etikettierung geben. Verleger zum Beispiel könnten eines Tages Bücher an Bibliotheken und Buchhandlungen ausliefern, die beschreibbare Etiketten haben. Jedes Exemplar von ›Die Früchte des Zorns‹ würde dann einen Teil seines Standard-Warencodes tragen, der mit dem auf jedem anderen Exemplar identisch ist. Die Bibliothek wird in der Lage sein, den restlichen Code anzupassen, so dass er ihren Anforderungen der Inventarkontrolle gerecht wird. Selbst wenn geschlossene Systeme geschlossen bleiben, macht ihr Mangel an Transparenz sie beunruhigend vom Standpunkt der Privatsphäre aus. Weil bestimmte Details über geschlossene Systeme möglicherweise nicht leicht erhältlich sind, hätten Konsumenten große Schwierigkeiten bei der Beschaffung der Informationen, die sie benötigen, um Gefährdungen ihrer Privatsphäre einschätzen und sich schützen zu können.« (FoeBuD, 2006)

Die Organisation benennt eine Reihe von Stadt- und Hochschulbibliotheken, die sich der RFID-Technik bedienen. In der Dokumentation ist ersichtlich, dass FoeBuD derzeit über die Hintergründe der Datenverwendung und Datenspeicherung in Bibliotheken wenig weiß. Dennoch wird an anderer Stelle pauschal behauptet:

> »Die Verarbeitung dieser Daten im großen Stil allerdings ermöglicht auch ›tolle‹ Interessenprofile auf Knopfdruck: ›Sag mir, was Du liest, und ich sage Dir, was Du denkst (und was Dich vielleicht verdächtig macht oder einen bestehenden Verdacht bestätigt).‹ Mit RFID in Büchern sind Gedanken nicht mehr frei.« (FoeBuD, 2011)

Kritisch äußert sich FoeBuD zu den Nutzerausweisen, insbesondere die mit Studentenausweisen kombinierte Variante in Hochschulbibliotheken (»die doch eigentlich die ›Hüterinnen des freien Geistes‹ sein sollten«). Auch hier werden zahlreiche Einrichtungen namentlich genannt. Außerdem erinnert die Website daran, dass der »Big Brother Award« 2004 für die Videoüberwachung in Hochschulen vergeben wurde.

> Immer mehr Universitäten und Fachhochschulen spicken ihre Studierendenausweise mit RFID. Ausgelesen werden die Chips meist in den Bibliotheken und in der Mensa, wenn die Studi-Ausweise in die Nähe des Lesegerätes gehalten werden.

> Fehlen nur noch die RFID-Lese-Antennen in den Türrahmen, dann heißt es »Ich weiß, welches Buch Du liest« – »Den Schein kriegst Du nicht, Du warst ja immer zu spät bei der Vorlesung« – »Ernähr Dich mal gesünder, dann schaffst Du auch Deine Prüfung…« usw. (FoeBuD, 2011)

Fachleute mögen diese Einlassungen als banal, unqualifiziert und sachlich falsch einstufen. Allerdings basierte auch die RFID-Kritik an Einzelhandel, Gesundheitseinrichtungen oder Staatsverwaltung auf Informationsdefiziten, Gerüchten und Schreckensszenarien. Fachexpertise der Kritiker entwickelte sich erst mit Recherchen und Aktionserfahrungen. Wesentlich ist, dass das Konfliktthema bereits entdeckt ist und gewisse Öffentlichkeit hat. Der RFID-Einsatz in ihren Ausweisen wird z. B. unter Studierenden und Studentenvertretungen diskutiert, wie sich in Blogs, Foren und Publikationen von Studentenvertretungen leicht feststellen lässt.

Auf der institutionellen Seite der Bibliotheken steht dem keine wirklich intensive Debatte über Datenschutz und Sicherheit gegenüber. Das hat mehrere Gründe: Die RFID-Einführung ist im Bibliothekswesen noch längst nicht flächendeckend und ein junges Thema, bei dem technische Fragen vorherrschen. Es gibt außer den allgemeinen Datenschutzbestimmungen kein RFID-spezifisches Recht, das zum Handeln zwänge. Verch (2007) betont, die rechtliche Bewertung sei von der technischen Ausgestaltung des RFID-Einsatzes abhängig. Allgemein werde eine begrenzte RFID-Technik bevorzugt, die auf passive Funkchips zur Identifizierung von Medien ohne datenschutzsensible Personendatenspeicherung setze, außerdem sei die Funkreichweite gering und spezielle Bibliothekssoftware zum Auslesen notwendig. Diese typische Argumentation habe »zu der vorherrschenden und durchaus bequemen Ansicht beigetragen, dass besondere datenschutzrechtliche Vorgaben beim Einsatz der RFID-Chips in Bibliotheken nicht zu beachten sind« (S. 2). Gleichwohl konstatiert Verch Missbrauchsgefahren, da die RFID-Bibliothekstechnik nicht losgelöst von kommerziellen Anwendungen und elektronischen Datenspuren im Alltag betrachtet werden könne. Sie meint:

> »In jedem Fall nimmt das Bibliothekswesen eine Vorreiterrolle in der Verbreitung der RFID-Technik in Deutschland ein und sollte dieser besonderen Verantwortung Rechnung tragen, indem es sich eng an datenschutzrechtlichen Leitlinien und ethischen Grundsätzen orientiert.« (Verch, 2007, S. 8)

Verch stellt der entspannten Haltung deutscher Bibliotheken die Kontroversen in den USA gegenüber. Sie verweist beispielsweise auf Protestdemonstrationen von Bürgern wie zur RFID-Einführung bei der San Francisco Public Library 2004, auf die grundsätzliche Ablehnung von RFID in Bibliotheken durch Bürgerinitiativen wie der Electronic Frontier Foundation (EFF) sowie auf die intensive Arbeit der American Library Assocation (ALA). Verch interpretiert die in Amerika verbreitete Sorge um den Schutz der Privatsphäre als Folge einer Politik, die Polizei und Geheimdiensten die Daten von Bibliotheksnutzern zugänglich macht – etwa durch Antiterrorgesetze nach 2001 wie dem Patriot Act. Die US-Bürger seien für das Thema Datenschutz in Bibliotheken besonders sensibilisiert, so Verch (S. 2).

Der Bibliotheksverband ALA habe – mit Berufung auf seinen Ethikkodex – gegen den Patriot Act Stellung bezogen und in Arbeitsgruppen allgemeine Datenschutzrichtlinien formuliert. Dazu gehören seit 2005 auch eine Verbandsresolution sowie Musterrichtlinien für den Einsatz von RFID, die Sicherheitsvorkehrungen gegen unbefugtes Datenauslesen fordern, den Verzicht auf die Speicherung von Personendaten auf Funkchips, umfassende Information der Bibliotheksnutzer über RFID, die Einführung hauseigener Datenschutzrichtlinien und regelmäßige Überprüfung durch externe Stellen. Vereinzelt sei die ALA von Bibliothekaren wegen ihrer Inflexibilität kritisiert worden. Verch sieht die ALA-Empfehlungen dennoch als Vorbild für Deutschland an. Hilfestellungen zum RFID-Datenschutz und zur RFID-Nutzerinformation seien Aufgaben für Bibliotheksverbände (S. 8).

Teilweise kursieren im Bibliothekswesen bereits Hilfestellungen durch Weitergabe vorbildlicher Bürgerinformationen einzelner Bibliotheken und Verbünde. Nach wie vor ist aber in den Verbänden und Arbeitsgemeinschaften die politische Auseinandersetzung mit RFID eine Randerscheinung. Nur gelegentlich thematisiert es die kleine Schar der Experten für Bibliotheksrecht.

Die fehlende kritische Haltung ist erklärbar: Für Bibliothekare erschließt sich der Nutzen der Technologie unmittelbar. Bibliotheken sind mit Handels- oder Logistikunternehmen vergleichbar, die an liberalen Rahmenbedingungen für die RFID-Einführung interessiert sind. Regulierungsauflagen wären für sie bürokratische Hemmnisse für RFID-Investitionen.

Berufsverbände und Gewerkschaften beschäftigen sich in erster Linie mit den internen Folgen der RFID-Einführung für das Bibliothekspersonal, vom Stellenabbaupotenzial über Gesundheitsschutz und Arbeitsplatzgestaltung bis zur Qualifizierung, von der Mitbestimmung und Mitarbeiterbeteiligung bei RFID-Projekten bis zu Betriebs- und Rahmendienstvereinbarungen. Das ist das vorrangige Interesse der Personal- und Betriebsräte. Eine Totalablehnung kann nicht festgestellt werden. Das Fazit einer Ver.di-Fachtagung 2009 in Berlin kam zu dem Schluss, RFID biete »mehr Chancen als Risiken« (Ver.di, 2009).

Dieser Fokus schließt den Blick über den Tellerrand nicht aus, wie sich z. B. bei Ver.di zeigt, einer Gewerkschaft, die ihr Mandat durchaus allgemeinpolitisch versteht und sich nicht auf die Funktionen eines »ADAC für Arbeitnehmer« zurückzieht, sondern z. B. auch Verbraucherinteressen einbeziehen will. Ver.di muss sich ohnehin mit RFID beschäftigen, da RFID im Handel eine wichtige Rolle spielt und es im Kontext des schnell wachsenden gewerkschaftlichen Arbeitsgebiets der Mitarbeiterüberwachung und der Forderung nach einem Beschäftigten-Datenschutzgesetz steht. Die Ver.di-Arbeitsgruppe RFID ist daher branchenpolitisch bei den Bundesfachgruppen Groß- und Einzelhandel angesiedelt, die dazu Betriebsrätekonferenzen und Publikationen initiiert hat (Ver.di, 2008).

In der bibliothekarischen Fachdiskussion sind in der Branchenpresse, in Verbänden und bei Fachkongressen kritische Einzelstimmen vernehmbar. Der Arbeitskreis kritischer BibliothekarInnen (Akribie) kam gar zu dem Schluss, die »bibliothekarische Ethik gebietet,

auf den Einsatz von RFID in öffentlichen Bibliotheken zu verzichten.« (Mahrt-Thomsen, 2010, S. 3). Mit Blick auf Fachkongresse monierte die Akribie-Aktivistin Frauke Mahrt-Thomsen, kritische Nachfragen zu RFID seien »weniger willkommen«, das Interesse liege eher darin, »die schöne neue Funk-Welt [...] in positiven Farben gemalt zu bekommen« (S. 1). Sie beklagt mangelnde Sensibilität für die rechtliche, ethische und politische Problematik. Neben den internen Folgen fürs Personal verweist sie auf mögliche Missbrauchs-Szenarien und Sicherheitsrisiken in verbreiteten RFID-Systemen, deren Verschlüsselung von Hackern geknackt werden könnten, aber auch Löcher in der Schutzkette durch die Zusammenarbeit mit Lieferanten, Wartungs- und Support-Dienstleistern. Sie kritisiert, dass der RFID-Einsatz in Bibliotheken die Verbreitung der Technologie legitimiere und Akzeptanz für die RFID-Industrie schaffe – hier müssten sich die Bibliothekare fragen lassen, ob sie den Vertrauensvorschuss der Nutzer nicht missbräuchten, wenn sie allzu bereitwillig auf die RFID-Technik umstiegen (S. 15). Datenschutzbeauftragte hätten es sich »nicht allzu schwer gemacht«, RFID-Anwendungen in Bibliotheken zu genehmigen. Sie hätten kaum eine rechtliche Handhabe und stünden unter dem Druck, als »Bedenkenträger« angefeindet oder in ihren Kompetenzen beschnitten zu werden, wenn sie sich bei Modernisierungsmaßnahmen quer stellten (S. 18).

Diese Positionen sind im Mainstream des Bibliothekswesens kaum verankert. Sie geben jedoch – im Sinne »schwacher Signale« – Konfliktherde wieder, die mit steigender RFID-Verbreitung Politik, Organisationen und Bibliotheksnutzer beschäftigen könnten.

Fazit: Politisches Risikomanagement für RFID-Projekte in Bibliotheken

Bibliotheken haben bei der Einführung und Entwicklung von RFID-Projekten auf das Potenzial von Konflikten mit ihren Stakeholdern zu achten. Das Projektumfeld beinhaltet Unwägbarkeiten und Bedrohungen. Diese Risiken und die relevanten Akteure mit ihrem Stör- aber auch Unterstützungspotenzial zu erkennen und zu analysieren, ist sowohl für die informelle Lobbyarbeit wie für formale Rechtsetzungsprozesse als auch die Öffentlichkeitsarbeit wichtig. Es gilt, die derzeit »schwachen Signale« zu erfassen und in die eigenen Fachdiskussionen und Strategieprozesse einzubringen.

Derzeit ist das Umfeld für RFID in Bibliotheken insgesamt eher als konfliktarm und freundlich zu bewerten, sieht man einmal von den Haushaltszwängen ab. Bleibt es so? Jedenfalls sollte gegenwärtig das Ziel – in Anschluss an Lobby-Strategieempfehlungen nach van Schendelen (2004, S. 174) – sein, die Lage so zu halten, wie sie ist. Praktisch bedeutet das, den Status quo durch die Gewinnung weiterer Unterstützer abzusichern und die positive Wahrnehmung der RFID-Projekte zu erhalten. Wenn möglich, sollten Entscheidungen über RFID forciert und das Tempo erhöht werden. Dabei sollten politisch brisante Thematiken wie der Datenschutz umsichtig bearbeitet, aber öffentlich zurückhaltend kommuniziert werden.

Sollte das Umfeld unfreundlicher werden, ist die Strategie anzupassen. In einer solchen Lage ist es nach van Schendelen nötig, in den Dialog mit Skeptikern und Kritikern einzutreten und sie soweit wie möglich einzubinden. Die negative Wahrnehmung der Projekte muss eingehegt, ein möglicher Schaden begrenzt werden. Setzt die Politik zu

Regulierungsaktivitäten an, sollten diese zeitlich gebremst werden. Dabei geht es nicht um Totalblockade, sondern um zeitliche Spielräume für erweiterte Diskussionen und Überzeugungsarbeit, möglichst unter Einbeziehung neuer Verbündeter und an die Interessenlage der Politik angepasster Argumente.

Der nächste Datenschutz-Skandal kommt bestimmt. Ob öffentliche Bibliotheken irgendwann maßgeblich davon betroffen sein werden, ist schwer vorherzusagen. Aber sie gehören zum Staatsapparat und sind schon deshalb ein leichtes Ziel für politische Angriffe. Ihre Technik ist ein Einfallstor für einen symbolischen Streit um gesellschaftliche Akzeptanz von RFID. Die Politik steht unter Druck, den Schutz von Daten und Bürgerrechten durchzusetzen, exemplarisch und symbolisch »im eigenen Haus« – auch und gerade lokal und regional. Gesellschaftlicher Widerstand würde die Bereitschaft der Politik zu hohen RFID-Investitionen bei Bibliotheken absenken.

Überdies haben Bibliotheken eine besondere Klientel, die ihnen einen hohen Vertrauensvorschuss gibt. Enttäuschung und Empörung können umso heftiger ausfallen. Bibliotheksnutzer könnten zum »Wutbürger« mutieren, die gegen moderne Technik und politisch-technokratische Bevormundung rebellieren, sich organisieren und auf die Politik Druck ausüben. Das muss nicht gleich eine nationale Bewegung sein: Auch lokal birgt RFID ein Saatkorn von Misstrauen und Zorn gegen Institutionen, die berechtigte Bürgersorgen nicht ernst nehmen. RFID-Projekte sollten auf Prävention achten.

Die RFID-Debatte wird auf allen politischen Ebenen fortgeführt. Selbstverpflichtungen der Wirtschaft dürften kurzfristig Standards fixieren. Langfristig sind auch gesetzliche Regeln zu erwarten. Dass eine neue Technologie flächendeckend eingeführt wird, ohne einer spezifischen, allmählich engeren Regulierung unterworfen zu werden, ist unwahrscheinlich. Dabei werden nicht nur deutsche und europäische Gesetzgeber aktiv werden, sondern auch die Gerichte. Das wird zu beobachten und auszuwerten sein.

Für die Strategie der Bibliotheken bleibt anzumerken, dass sie mit guter Praxis bei Datenschutz und Informationspolitik Konflikte um RFID überstehen können. Wenn sie den politischen Dialog ernstnehmen, Transparenz zeigen, sich eigene sensible Regeln geben und Ethik-Fragen nicht ausweichen, liegen die Chancen nicht schlecht. Das gilt auch für den Anspruch, per Lobbying künftige Gesetze zu RFID mitgestalten zu wollen – ein Anspruch, den Bibliotheken und ihre Verbände laut und klar erheben sollten.

Literaturverzeichnis

American Library Association. (2011). Advocating in a Tough Economy Toolkit. Abgerufen am 17. August 2011 von ALA Issues & Advocacy: http://www.ala.org/ala/issuesadvocacy/advocacy/advocacyuniversity/toolkit/index.cfm

Bundesministerium des Innern. (14. Mai 2009). Dritter Bericht des BMI über die Sponsoringleistungen an die Bundesverwaltung. Abgerufen am 29. August 2011 von http://www.bmi.bund.de/SharedDocs/Downloads/DE/Veroeffentlichungen/dritter_sponsoringbericht.pdf?__blob=publicationFile

Bundesministerium für Wirtschaft und Technologie. (Juli 2007). European Policy Outlook RFID. Abgerufen am 3. August 2011 von http://www.nextgenerationmedia.de/documents/European_Policy_Outlook_Paper_RFID_Finale_Version_dt..pdf

Denkler, T. (31. Juli 2007). Der gesponserte Staat. Abgerufen am 12. August 2011 von Sueddeutsche.de: http://www.sueddeutsche.de/politik/bericht-der-bundesregierung-der-gesponserte-staat-1.785742

Deutscher Bibliotheksverband. (14. September 2010). Bibliotheksverband schlägt Alarm: zwei Drittel aller kommunalen Bibliotheken von Einsparungen betroffen, Pressemitteilung. Abgerufen am 2. Juni 2011 von http://www.bibliotheksverband.de/fileadmin/user_upload/DBV/pressemitteilungen/2010/2010-09-14_PM_Finanzlage_01.pdf

Deutscher Bundestag. (23. Januar 2008). Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie, Drucksache 16/7891. Abgerufen am 21. August 2011 von http://dipbt.bundestag.de/dip21/btd/16/078/1607891.pdf

Deutscher Bundestag. (15. August 2011). Dokumentations- und Informationssystem (DIP), Dokumentensuche »RFID«, 16. Wahlperiode. Abgerufen am 15. August 2011 von Deutscher Bundestag: http://dipbt.bundestag.de/dip21.web/searchDocuments/simple_search.do

Deutscher Bundestag. (6. Januar 2010). Unterrichtung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung: Technikfolgenabschätzung (TA) Zukunftsreport Ubiquitäres Computing, Drucksache 17/405. Abgerufen am 2. August 2011 von http://dipbt.bundestag.de/dip21/btd/17/004/1700405.pdf

Europäische Kommission. (12. Mai 2009a). Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen, K(2009) 3200. Abgerufen am 22. August 2011 von http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF

Europäische Kommission. (18. Juni 2009b). Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 18. Juni 2009 über das Internet der Dinge – ein Aktionsplan für Europa (KOM(2009)0278). Abgerufen am 22. August 2011 von http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:DE:PDF

Europäischer Gerichtshof. (9. März 2010). Urteil des Gerichtshofs (Große Kammer) Vertragsverletzung eines Mitgliedstaats – Richtlinie 95/46/EG – in der Rechtssache C518/07. Abgerufen am 9. August 2011 von http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=de&num=79899690C19070518&doc=T&ouvert=T&seance=ARRET

Europäisches Parlament. (15. Juni 2010). Entschließung des Europäischen Parlaments vom 15. Juni 2010 zu dem Internet der Dinge (2009/2224(INI)), P7_TA(2010)0207. Abgerufen am 5. August 2011 von http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0207&language=DE

FoeBuD. (2011). Big Brother Awards. Abgerufen am 23. August 2011 von http://www.bigbrotherawards.de/

FoeBuD. (15. Oktober 2008). Die Gewinnerinnen und Gewinner des Wettbewerbs für ein RFID-Warnlogo. Abgerufen am 23. August 2011 von http://www.foebud.org/rfid/rfid-warnlogo-wettbewerb/die-gewinnerinnen-und-gewinner-des-wettbewerbs-fuer-ein-rfid-warnlogo/

FoeBuD. (28. Januar 2006). Schnüffelchips: RFID-Industrie setzt auf PR-Offensive statt auf konstruktiven Dialog. Abgerufen am 10. Juli 2011 von FoeBuD: http://www.foebud.org/rfid/schnueffelchips-rfid-industrie-setzt-auf-pr-offensive-statt-auf-konstruktiven-dialog/

FoeBuD. (29. Dezember 2006). Unsere Positionen. Abgerufen am 25. August 2011 von http://www.foebud.org/rfid/unsere-positionen

FoeBuD. (2011). Wo gibt es RFID? Abgerufen am 15. August 2011 von http://www.foebud.org/rfid/wo-gibt-es-rfid

Hamann, G. (19. Januar 2006). Chip, Chip, hurra? Datenschützer kontra Handel – der Streit um die Zukunft der RFID-Funktechnologie eskaliert. Abgerufen am 15. Juli 2011 von Zeit online: http://www.zeit.de/2006/04/RFID/komplettansicht

Huber, A. (10. August 2007). Koalitionen und Strategische Allianzen: Praxis der Bildung und Steuerung. Berlin: Deutsches Institut für Public Affairs.

Informationsforum RFID. (2009d). »Die Debatte bleibt aktuell«. Abgerufen am 22. August 2011 von RFID Special: Fünf Jahre Informationsforum RFID: http://info-rfid.de/info-rfid/content/e107/e127/e781/jahresbericht_2009_ger.pdf

Informationsforum RFID. (1. April 2008a). Informationsforum RFID und ORACLE setzen bundesweite RFID-Veranstaltungsreihe für kleine und mittlere Unternehmen fort. Abgerufen am 2. August 2011 von Presseportal.de: http://www.presseportal.de/pm/59187/1164084/informationsforum-rfid-und-oracle-setzen-bundesweite-rfid-veranstaltungsreihe-fuer-kleine-und

Informationsforum RFID. (5. Mai 2009). Mittelstandspreis RFID 2009 – jetzt bewerben. Abgerufen am 5. August 2011 von Presseportal.de: http://www.presseportal.de/pm/59187/1399601/mittelstandspreis-rfid-2009-jetzt-bewerben

Informationsforum RFID. (2011). Positionspapiere 2006-2009. Abgerufen am 29. August 2011 von http://info-rfid.de/publikationen/positionspapiere/index_ger.html

Informationsforum RFID. (2009c). RFID Special: Fünf Jahre Informationsforum RFID. Abgerufen am 22. August 2011 von http://info-rfid.de/info-rfid/content/e107/e127/e781/jahresbericht_2009_ger.pdf

Informationsforum RFID. (Oktober 2008b). RFID zeigt Gesicht! Wettbewerb. Abgerufen am 10. August 2011 von http://info-rfid.de/info-rfid/content/e107/e127/e230/rfid_beileger_logowettbewerb_ger.pdf

Kümmerlen, R. (10. März 2009). Initiative soll RFID voranbringen. Abgerufen am 22. August 2011 von Deutsche Verkehrs-Zeitung: http://www.dvz.de/nc/en/news/alle-news/einzelseite/id/initiative-soll-rfid-voranbringen.html

LobbyControl. (22. September 2005). FIFA und Metro gegen ZDF-Bericht über RFID-Funkchips. Abgerufen am 29. Juli 2011 von LobbyControl: http://www.lobbycontrol.de/blog/index.php/2005/09/fifa-und-metro-gegen-zdf-bericht-ueber-rfid-funkchips/

Mahrt-Thomsen, F. (25. Februar 2010). RFID – moderne Technik mit Tücken. Abgerufen am 22. März 2011 von Staatsbibliothek zu Berlin, Fachtagung der Virtuellen Fachbibliothek Recht und der Arbeitsgemeinschaft für juristisches Bibliotheks- und Dokumentationswesen : http://www.vifa-recht.de/fachtagung2010/download/Vortrag_Mahrt-Thomsen_Web.pdf

MUFV & Landesbeauftragterfür den Datenschutz. (2010). RFID Radiofrequenzidentifikation: Was ist das? Informationsbroschüre. Mainz: Ministerium für Umwelt, Forsten und Verbraucherschutz und Landesbeauftragterfür den Datenschutz Rheinland-Pfalz.

MUFV. (7. September 2010). Conrad und Wagner: »Funktechnologie RFID braucht Kennzeichnung und Transparenz – Broschüre informiert«. Abgerufen am 3. August 2011 von Ministerium für Umwelt, Forsten und Verbraucherschutz: http://www.mulewf.rlp.de/aktuelles/einzelansicht/archive/2010/september/article/conrad-und-wagner-funktechnologie-rfid-braucht-kennzeichnung-und-transparenz-broschuere-inf/?Fsize=1&cHash=7d199a7afb9128e23b840ae9b1373d0b

Quack, K. (6. März 2009). EU ergreift die RFID-Initiative. Abgerufen am 19. August 2011 von Computerwoche.de: http://www.computerwoche.de/software/erp/1889319/

Ratzek, W. (2010). So funktioniert Lobbyarbeit – Beispiele aus der Praxis. In W. Ratzek, Lobbyarbeit für Information Professionals: Grundlagen – Beispiele – Empfehlungen (S. 11-36). Bad Honnef: Bock + Herchen.

Rawe, S., & Schulz, J. (2005). Issues Management. In S. Rawe, M. Althaus, & M. Geffken, Handlexikon Public Affairs (S. 111-114). Münster und Berlin: Lit.

RFID im Blick. (4. März 2011). Quo Vadis Informationsforum RFID? Abgerufen am 20. August 2011 von RFID im Blick: http://www.marktplatz-rfid-im-blick.de/201103042827/quo-vadis-informationsforum-rfid.html

Stegherr, M. (Dezember 2005a). Die Lobby im Schnellboot. Politik & Kommunikation , S. 46-48.

Stegherr, M. (Dezember 2005b). Regulierung zerstört Ansätze. Politik & Kommunikation , S. 49.

van Schendelen, R. (2004). Machiavelli in Brussels: the art of lobbying the EU. Amsterdam: Amsterdam University Press.

Ver.di. (Juli 2009). Fachtagung Bibliotheken am 12. Juni 2009 in Berlin RFID in Bibliotheken – mehr Chancen als Risiken. Abgerufen am 18. Juli 2011 von http://gemeinden.bb.verdi.de/berlin_-_fb_7/fk_bibliotheken

Ver.di. (20. August 2008). Radio Frequency Identification (RFID) – menschengerecht gestalten. Abgerufen am 15. Juli 2011 von http://handel.verdi.de/branchenpolitik/rfid

Verch, U. (16. April 2007). Selbstklebend, selbstverbuchend und auch selbstverpflichtend? Rechtliche Rahmenbedingungen für den Einsatz von RFID-Chips in Bibliotheken. Vortrag, Bibliothekskongress Leipzig. Abgerufen am 15. August 2011 von Berufsverband Information Bibliothek: http://www.opus-bayern.de/bib-info/volltexte/2007/305/pdf/verch-leipzig-2007.pdf

von Münchow, A. (Frühjahr 2006). Strategische Allianzen: Effektivere Lobbyarbeit für Verbände und Unternehmen durch Koalitionen. Public Affairs Manager , S. 38-45.

Wiebusch, D. (2005). Strategische Allianzen. In M. Althaus, S. Rawe, & M. Geffken, Handlexikon Public Affairs (S. 217-220). Münster und Berlin: Lit.

Bibliotheken sind »smart« geworden
Ein Plädoyer für ein bewusstes »smart« machen in den nächsten Jahren

Frank Gillert

Vor mehr als zehn Jahren haben RFID-Systeme Einzug in die deutsche Bibliothekswelt gehalten. Heute kann konstatiert werden, dass rund 1000 öffentliche und wissenschaftliche Einrichtungen damit ausgestattet und rund 20 Millionen Medien »smart geworden« sind. Der folgende Beitrag soll auf Basis des Innovations- und Technologiemanagements aufzeigen, welche Mechanismen zu dieser Entwicklung geführt haben und welche Erkenntnisse für eine weitere, bedarfsorientierte Technologisierung des Bibliothekswesens daraus gezogen werden können; für ein bewusstes »smart« machen.

Einleitung

Dieses Buch beinhaltet, nahezu vollständig, den Facettenreichtum des RFID-Einsatzes in Bibliotheken. Es werden Entwicklung, Status und zukünftige Trends auf das Tableau gebracht. Darunter sind jedoch einige Beiträge, die es – ungeachtet ihrer inhaltlichen Qualität – nicht geben müsste, wenn die Anfangsjahre bewusster gestaltet worden wären. Es ist nicht ein Phänomen, das nur in Bibliotheken bekannt ist, sondern ein Phänomen der Zeit. Alle Lebensbereiche unterliegen einer beschleunigten Technologisierung, privat, unternehmerisch, eben gesamtgesellschaftlich. Die Zyklen der Erneuerung werden weiterhin kürzer werden. Die fortschreitende Miniaturisierung von Elektronikkomponenten, die positive Preisentwicklung, der Ausbau der Breitbandkommunikationsverbindungen und insbesondere die digitale Konvergenz von Geräten und Diensten sowie die Konvergenz von gewerblichen und privaten Nutzungsprofilen mobiler Endgeräte (Stichwort Bring your own Device) sind nicht mehr nur als Trends auszumachen. Sie sind Fakten einer Mobilen Gesellschaft. Auch das Thema Cloud Computing ist gekoppelt mit der Nutzung mobiler Endgeräte, da durch die Verlagerung von Daten und Software Services die Endgeräte selber noch mehr Applikationen auf kleinstem Raum aufweisen können. Die Entwicklungsgeschwindigkeit von insb. Informations- und Kommunikationstechnologien sind extrem hoch und die digitale Konvergenz führt zur Aufweichung von Systemgrenzen und damit zur Verschmelzung von Inhalten. Dabei geht die informationelle Selbstbestimmtheit durch die Selbstvernetzung der Geräte zunehmend verloren.

Damit berührt das Technologiemanagement als Disziplin immer weitere Kreise. War es zuvor den Technologieexperten überlassen, handeln heute immer mehr Akteure, privat wie beruflich, professioneller im Zusammenhang mit Technologieentscheidungen. Die Debatte um den Datenschutz und die Datensicherheit ist Ausdruck eines Unbehagens gegenüber der Komplexität und in der Sicherheitsforschung wird längst nicht mehr auf das Verdikt der Technologieexperten gesetzt. Dabei wurde deutlich, dass der Versuch, eindimensionale, lineare Kausalketten zu definieren und zu bewerten zunehmend

scheiterte, die die wissenschaftlichen Einzeldisziplinen disjunkt zu behandeln suchten. Es wurde deutlich, dass der gesellschaftliche Diskurs, die Beteiligung der »Laien« eine Mehrdimensionalität in die Risikobewertung gebracht hat, die der Subjektivität, d. h. der gerechtfertigten, individuellen Wahrnehmung von Risiken, gerecht wurde. [1, S.32 ff.] Vor diesem Hintergrund erhält der Begriff systemische Risiken Einzug in die Diskussion [2, S.21 und die dort zitierte Literatur].

Die Festlegung eines gesellschaftlich tragbaren Restrisikos für einen Technologieeinsatz ist heute politisch nicht mehr legitimiert. Damit steigen aber auch die Verantwortung des Einzelnen und die Notwendigkeit um die komplexen Sachverhalte zu wissen und sie zu bewerten. In Bezug auf den Einsatz von RFID in Bibliotheken ist die Entscheidung über den Einfluss auf den Datenschutz der Akteure selbst zu bewerten und damit auch zu verantworten. Die Europäische Kommission hat dazu ein umfängliches Procedere[1] geschaffen, das vor dem Hintergrund der Selbstverpflichtung der öffentlichen und privatwirtschaftlichen Nutzung von RFID (und auch NFC) die Folgeabschätzung in die Hände der Akteure legt.

Damit ist der Kompetenzerwerb für das Management von Technologien in Bibliotheken präjudiziert. Dennoch ist nicht alleine die Fragestellung den Schutz der Personen betreffend zu beantworten, um somit die notwendige Akzeptanz für den Erfolg des Einsatzes zu gewährleisten; auch das Verständnis bezogen auf die Vorteilhaftigkeit der Investition muss vorhanden sein. Im Zusammenhang mit dem Technologiemanagement ist nicht nur der Return on Invest (ROI) oder die Amortisationszeit gemeint, sondern auch der Investitionsschutz durch die richtige Wahl einer Technologie. Damit wird mit dem technologiezentrischem Wissensmanagement ein dritter, ohnedies originärer Kompetenzbereich von Bibliotheken adressiert. Woher bekomme ich in Qualität und Aktualität verlässliche Informationen? Zudem soll das gegenseitige Verständnis von Technologieanbietern und Anwendern verbessert werden, um Innovationen zum Vorteil beider Seiten gestalten zu helfen. Dieser Beitrag hat zum Ziel, Handlungsempfehlungen für den Einsatz von neuen Technologien und Konzepten zu geben, wobei RFID Gegenstand und gleichzeitig Präzedenzfall ist.

Zur Genese des RFID-Marktes oder wurde »auf das richtige Pferd gesetzt«

Vom Technology Push zum Demand Pull

Ein erklärtes Ziel des Innovationsmanagements [vgl. 3] ist die Zusammenführung von Technology Push und Demand Pull. Das bedeutet, die Anforderungen der Bedarfsträger werden in Form einer Lastenbeschreibung technologieunabhängig formuliert und mit technologischen Entwicklungen im Sinne von Erfindungen abgeglichen. Im Idealfall werden die Entwicklungen darüber erst angestoßen. In der Realität wird jedoch der Prozess umgekehrt, wobei (zufällige) Technologieentwicklungen nach passenden Problemen auf Seiten der Bedarfsträger suchen. Will man diese Zusammenhänge vermitteln, bietet sich die RFID-Technologie als multi-perspektivisches Beispielkonstrukt an. Vieles

1 vgl. Kapitel von Verch, Ulrike: »Datenschutzrechtliche Bedenken beim Einsatz von RFID-Technologie aus europäischer Perspektive zu Privacy Impact Assessment (PIA)«

von dem was die Theorie von Innovations- und Technologiemanagement zu vermeiden versucht, lässt sich plakativ am Beispiel RFID zeigen.[vgl. 4, S.7-S.43]

Mit der Entwicklung der Smart Label in den frühen 1990ziger Jahren wurde der Grundstein für ein Jahrzehnt exorbitanter »Problemsuche« eingeläutet, die mit dem Start des AutoID Centers in den USA 1999 und nachfolgend der Gründung des epcglobal Konsortiums zu der bekannten Hype-Situation geführt hat. Vor dem Hintergrund einer in weiten Kreisen akzeptierten Henne-Ei Konstellation zwischen Stückpreisanforderungen und eingesetzten Smart Label Mengen wurde auf Seiten der Technologieanbieter vehement in das Geschäftsfeld RFID investiert. Der quartäre Wirtschaftssektor von Konferenzveranstaltern und Marktanalysten heizte mit herausragenden Marktwachstumszahlen das Klima weiter an. Trotz aller Anstrengungen konnten die Implementierungsziele inbs. im Handel nicht erreicht werden. Ab etwa 2007 ist dann interessant zu verfolgen, wie diese Zahlen sukzessive nach unten korrigiert wurden. Investitionen in Geschäftsfelder wurden zurückgefahren oder sie wurden gänzlich geschlossen.

Die Analyse von Technologieadaptionsprozessen wird jährlich seitens der Gartner Group[2] im Rahmen des Gartner Hype Cycles unterstützt. Hierin findet sich neben der Nennung der Technologien auch deren Marktreife. Abbildung 1 zeigt den qualitativen Verlauf und die von Gartner definierten Phasen. Eine Diskussion der RFID-Technologie der Jahre 2005/2006 findet sich z. B. in [4, S. 12].

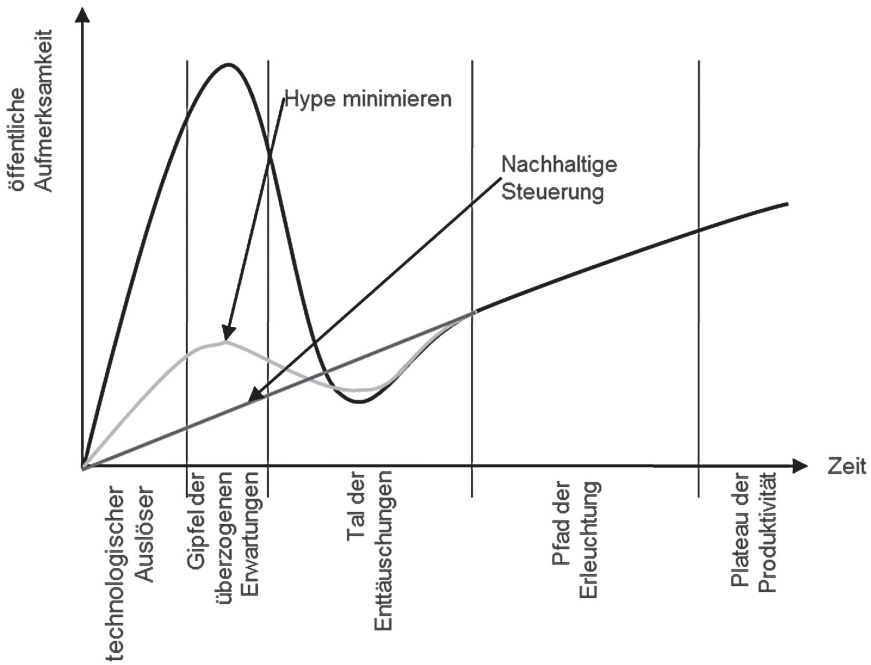


Abbildung 1: Rahmenbedingungen für RFID-Einsatz (in Anlehnung Gartner Hype Cycle[3])

2 Gartner Group: http://www.gartner.com

3 ebenda

Wie in Abbildung 1 dargestellt kann die Einführung von Technologien auch nachhaltig gesteuert werden, so dass eine extreme Ausbildung des »Gipfels überzogener Erwartungen« vermieden wird und damit auch das »Tal der Enttäuschungen« weitaus flacher ist.

Was bedeutet das für den Einsatz von RFID in Bibliotheken. Nachdem die RFID-Industrie in den »Killer-Applikationen« im Handel nicht die gewünschten Wachstumserfolge erzielen konnte, wurde die Suche nach sogenannten »low hanging fruits« gestartet. Das bedeutet, die Komplexitätsbarriere bzw. Kostenbarriere zum Einsatz von RFID ist nicht hoch und es entstehen Referenzprojekte für die Technologie selber oder einfach Umsätze für einen Geschäftsbereich, bzw. Unternehmen. In Abbildung 2 sind die Implementierungsbarrieren dargestellt. Vor dem Hintergrund einer langjährigen Verwendung der Etiketten, verteilen sich die initialen Kosten auf eine Vielzahl von Geschäftsvorgängen und die geschlossene Anwendung innerhalb einer Bibliothek benötigt nicht zwangsläufig mit anderen abgestimmte Standards.[4]

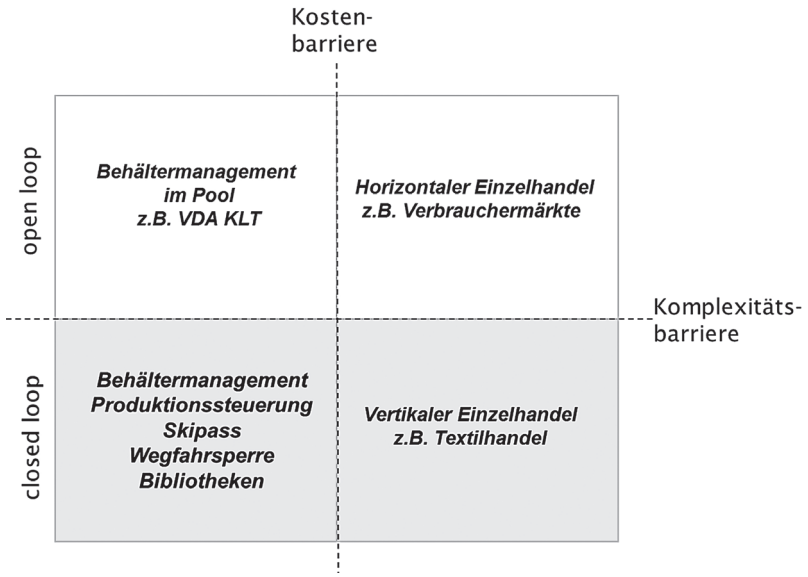


Abbildung 2: Rahmenbedingungen für RFID-Einsatz (in Anlehnung [4, S. 40])

Im Jahr 2001 wurde in Siegburg die erste Bibliothek mit RFID ausgestattet[5]. Dabei wurde auf Basis von im Markt verfügbaren unspezifischen Lesegeräten in Kombination mit einer dafür erstellten Software eine Lösung »gebastelt«. Die Notwendigkeit Leuchtturmprojekte auf Basis RFID zu generieren, führte bereits in den frühen Jahren zu verhältnismäßig niedrigen Etikettenpreisen, in deren Folge Anbieter von Etiketten sich aus dem Geschäft zurückgezogen haben. Die aus Sicht eines Etikettenherstellers geringe Stückzahl pro Fertigungslos hat auf Basis der Zielpreise wenig Raum für Geschäftsmodelle gelassen.

4 das dies dennoch der Fall ist liegt hauptsächlich in den Stückkosten bei großen Mengen gleichartiger Komponenten

5 Der Autor war Projektleiter von Siegburg, Stuttgart und Wien auf der Anbieterseite in den Jahren 2001-2003

Die Entwicklung der RFID-Technologie ist daher geprägt durch den ständigen Konflikt um Funktionalität und Kosten. Bei sicherheitsrelevanten Applikationen im Bereich der Personenidentifikation überwiegt maßgeblich die Forderung nach Datensicherheit und Datenschutz und führt zu einem hohen Grad an »Security by Design« unter Nutzung komplexer Hardwarelösungen. Im Gegensatz dazu haben sich prozessorientierte Anwendungen wie Bibliotheken im Wesentlichen über die zwei folgenden Faktoren entwickelt:

- Einfachheit der Architektur der RFID Chips zur Kostenminimierung
- Weitreichende offene Standards zur Aktivierung des Economy of Scale und damit Erreichung attraktiver Stückkosten für RFID Tags

Zusätzlich lassen sich Differenzierungsmerkmale durch Qualitätsunterschiede schwer vermitteln. Spezifische Technische Richtlinien, wie sie im industriellen Umfeld die Grundlage von Systemspezifikationen bilden, waren bis zum Jahr 2012 in Bibliotheken nicht vorhanden. Mit der VDI Richtlinie 4478[6] ist dies erstmalig gelungen. Die Richtlinie schlägt die Brücke zwischen den Geschäftsmodellen der Anbieter und den Anforderungen der Bibliotheken im Rahmen der öffentlichen Vergabe, indem Qualitätsunterschiede messbar werden. Dieser Weg sollte weiter beschritten werden. Das bestehende Richtlinienblatt 4478-1 beschreibt RFID Gatesysteme und sollte durch weitere Komponentenbeschreibungen, insb. Etiketten, ergänzt werden. Dies gelingt dann, wenn die Interessenvertreter der Bibliothekare auf der Verbandsseite das Thema institutionalisieren.

Als Fazit kann festgehalten werden, dass RFID-Lösungen in Bibliotheken nicht durch den Einsatz anforderungsgerechter, sondern verfügbarer Komponenten geprägt ist. Unzureichende zukunftsorientierte Anforderungsbeschreibungen lassen weiterhin Raum für Technologieanbieter, Bibliotheken als »Testbed« zu betrachten, anstatt zielorientierte Road-Maps zu entwickeln. Der Status Quo in Bezug auf die Zielpreise hemmen zudem Innovationen, weil bezogen auf die potenzielle Marktgröße aus Sicht von entwicklungsorientierten Unternehmen robuste Geschäftsmodelle nur schwer darzustellen sind.

Die Gestaltung der Zukunft oder Bibliothekare als Innovationsmanager

Wie eingangs beschrieben, werden die Technologiezyklen kürzer. Die Grundlage ist auch weiterhin das Moore'sche Gesetz, nachdem alle 18 Monate eine Verdopplung der Leistung in der Mikroelektronik erfolgt. Die damit verbundenen Potenziale zum Einsatz innovativer Technologien nehmen damit zu. Diese Potenziale bewirken grundlegende gesellschaftliche Veränderungen, die wiederum Bibliothekskonzepte maßgeblich beeinflussen. Es gilt nun diese Dynamik pro-aktiv zu nutzen, indem Szenarioanalysen mögliche Zukünfte beschreiben helfen. Damit können Anforderungen an den zukünftigen Technologieeinsatz der Zukunft formuliert und Entwicklungsplanungen seitens der Systemanbieter unterstützt werden.

Die Systemanbieter sind naturgemäß gewohnt, Innovationsprozesse professionell zu managen. Je nach Unternehmenskultur nimmt das Innovationsmanagement mehr

6 vgl. Kapitel von Zissel, Gillert: »Qualitätsbestimmung von RFID-Komponenten auf der Basis von allgemein anerkannten Normen und Richtlinien – Vereinfachung von Ausschreibungen«

oder weniger Raum ein. Ein jedes Unternehmen startet jedoch Entwicklungsprozesse, wenn die Marktchancen gegeben sind und ein Geschäftsmodell vorliegt. Hier gilt es das Verständnis für Geschäftsmodelle seitens der Kunden zu schärfen. Zuweilen ist für Anwender nicht nachzuvollziehen, dass trotz größerer Abnahmemengen, angemessener Preise und ggf. der Übernahme der Entwicklungskosten, dennoch von der Entwicklung Abstand genommen wird. Hier kann der Grund z. B. in anderen Opportunitäten, für die es sich eher lohnt, die Entwicklungskapazitäten zu binden.

Darüber hinaus ist die genaue Beschreibung der Anforderungen derart erforderlich, dass es von Technologienentwicklungsfirmen verstanden wird. Damit sind die spezifische Struktur und der Duktus der Dokumente gemeint.

Der zurzeit existierende Technologieradar[7] an der ETH Zürich und Fachhochschule Potsdam könnte eine Rolle in der Zukunft spielen, zeigt sich aber eher leblos[8]. Es ist ohnedies davon auszugehen, dass die Institutionalisierung eines technologiestrategischen Kreises eine zentrale, an die Leitung gebundene Struktur benötigt. Zudem müssen die Ziele eines »Think Tanks« klar formuliert werden und im Rahmen von Prozessen abgebildet sein. Die hier angeführten Handlungsempfehlungen können einen Kondensationskeim für die Strukturierung bilden.

Handlungsempfehlungen für einen zentralen Bibliotheks Think Tank:

1. Willensbekundung und aktive Unterstützung der Leitung der Interessenvertretung von Bibliotheken
2. Szenarienentwicklung für zukünftige Bibliothekskonzepte
3. Zielgerichtetes und kontinuierliches Monitoring von Technologieentwicklungen
4. Kompetenzaufbau für Technologiebewertung und Technologiefolgebewertungen
5. Klassifizierung von Einsatzfeldern/Nutzen
6. Frühzeitige Erstellung von Lastenheften zur Motivation von Innovationen
7. Frühzeitige Erstellung von technischen Beschreibungen (Richtlinien) parallel zu einer Pilotstellung, um die Migration in die Ausschreibungen zu erleichtern

Wenn es gelänge, eine zentrale Anlaufstelle für Technologieanbieter zu schaffen, die einen echten Mehrwert für die Innovationsprozesse bietet, wird aus der Reaktion auf Entwicklungen Aktion und Gestaltungskompetenz.

Fazit

Seit Beginn des RFID-Einsatzes hat sich viel getan. Die Lösungen sind gereift und funktional ansprechend. Dennoch sind Innovationen in diesem Gebiet weiterhin rar. Dazu müssen Anforderungen klar formuliert und Leistungsunterschiede klar nachgewiesen werden. Damit verbunden, muss auch die Bereitschaft vorhanden sein, die Leistungen angemessen zu honorieren. Sollten dann die Geschäftsmodelle dennoch

7 http://technologieradar.elgg.com/

8 Aufruf Homepage 19.12.2012. Letzter Eintrag Neueste Aktivitäten »12 month ago«

nicht erfolgreich sein, kann auch dies klar formuliert werden. Im Prozessumfeld (insb. Handel/Industrie) wird zurzeit die UHF-Technologie[9] maßgeblich präferiert, wodurch auch eine Rückkoppelung mit den Bibliotheken entsteht. Gerade im Hinblick auf eine erhoffte Verbesserung der Inventurprozesse. Bezogen auf die in letzten Abschnitt empfohlenen Maßnahmen, sollte eine noch gerade frühzeitige Technologiemanagementbetrachtung erfolgen. Aber RFID ist längst nicht die alleinige Herausforderung; es kommen schnell neue, interessante und nutzenversprechende Technologien – von Ortung und Lokalisierung, über mobile Endgeräte mit Apps, bis zur cloud – für die die Bibliotheken ihre nutzenstiftenden Anforderungen definieren müssen.

Literatur

[1] Evers, Adalbert, Nowotny, Helga: »Über den Umgang mit Unsicherheit: Die Entdeckung der Gestaltbarkeit der Gesellschaft«, Suhrkamp, Frankfurt am Main, 1987

[2] Renn, Ortwin: »Risiko: Über den gesellschaftlichen Umgang mit Unsicherheit« Oekom Verlag, München, 2007

[3] Hauschildt Jürgen, Salomo, Sören: »Innovationsmanagement«, Verlag Franz Vahlen München, 5. Auflage, 2011

[4] Gillert, Frank, Hansen, Rüdiger: »RFID für die Optimierung von Geschäftsprozessen«, Verlag Hanser München, 2006

9 vgl. Kapitel von Weinländer, Markus, Horst, Dieter: HF oder UHF – Welche Frequenz darf es sein? Vor- und Nachteile der gängigen RFID-Technologien

HF oder UHF – Welche Frequenz darf es sein?
Vor- und Nachteile der gängigen RFID-Technologien

Markus Weinländer, Dieter Horst

Die Frage nach der Funkfrequenz eines Radio-Frequency-Identification-Systems (RFID-Systems) ist in etwa wie die Frage nach der PS-Zahl eines Autos: Eigentlich keine primäre Kennzahl für den Anwender wie Höchstgeschwindigkeit oder Beschleunigungsverhalten, aber aufgrund ihrer technischen Bedeutung trotzdem maßgeblich. Ähnlich verhält es sich bei RFID: Zwar stehen eigentlich Eckdaten wie Reichweite, Speicherkapazität oder auch Kosten im Vordergrund. Doch die verwendete Frequenz ist so bedeutend für die Eigenschaften eines RFID-Systems, dass man auch als reiner Anwender kaum an der Frage »HF oder UHF?« vorbei kommt.

Aufbau von RFID-Systemen

RFID-Systeme bestehen aus drei Hauptkomponenten: einem Transponder mit integrierter Antenne, einem Schreib-/Lesegerät (»Reader«) und einer zugehörigen Sende- und Empfangsantenne. Die Transponder sind Datenträger mit mehr oder weniger Speicherkapazität, die über Funkwellen gelesen und auch beschrieben werden. Häufig sind die Transponder nicht nur lesbar, sondern können auch beliebig oft umprogrammiert (beschrieben) werden. Eine weitere Unterscheidung bezieht sich auf die Energieversorgung: Meist entnehmen die Transponder die gesamte benötigte Energie aus dem elektrischen Feld des Schreib-/Lesegeräts und können deshalb auf eine Batterie verzichten (passiv). Für höhere Reichweiten oder Speicherkapazitäten kann es hingegen notwendig sein, eine Stützbatterie für die Speicherbausteine und die Verarbeitungslogik, nicht aber für die Datenkommunikation einzusetzen (semi-aktiv). Schließlich gibt es auch aktive Transponder, die die eigene Batterie auch zum Senden verwenden; solche Komponenten kommen meist nur in Spezialanwendungen zum Einsatz.

Das Lesegerät samt der zugehörigen Antenne bezeichnet man als Erfassungsstelle. Während die Antenne nur die Funksignale aussendet und empfängt, bildet das Lesegerät eine Art Funkgerät, d. h. die Signale auf der Luftschnittstelle werden in digitale Informationen übersetzt und über geeignete Schnittstellen (z. B. Ethernet) an überlagerte Software-Systeme übergeben. Das Lesegerät liefert über die Antenne die benötigte elektrische Energie für den Betrieb der (passiven) RFID-Transponder; gleichzeitig erfolgt über diese sog. Luftschnittstelle auch die Datenkommunikation nach definierten Protokollen. Die praktische Ausführung einer RFID-Erfassungsstelle kann sehr unterschiedlich ausfallen: von kleinen Lesegeräten mit integrierter Antenne bis zu sog. Portalreadern, die mehrere Antennen einsetzen.

Kriterien für RFID-Systeme

Aus Anwendersicht wäre, wie eingangs geschildert, die Frequenz eigentlich unwichtig, würde sie nicht in erheblichem Maß die technischen Eigenschaften bestimmen. Wesentliche Parameter für konkrete Anwendungen sind vielmehr der maximale Lese-/Schreibabstand (Reichweite), die mögliche Speichergröße sowie weitere Eigenschaften wie die Pulkfähigkeit oder unterstützte Standards.

Der gewünschte Lese-/Schreibabstand der Transponder zu den Erfassungsantennen kann zwischen wenigen Zentimetern bis zu mehreren Metern reichen. Allerdings ist hier Vorsicht geboten, denn bei reichweitenstarken Geräten kann es auch rasch zu Überreichweiten kommen: Hier werden Transponder erfasst, die eigentlich gar nicht ausgelesen werden sollen. Die Folgen sind fatal: Wenn z. B. bei einer Anwendung zur Zutrittskontrolle auch andere, weiter entfernte RFID-Chips erfasst würden, so könnte sich jemand unbefugten Zutritt verschaffen.

Sowohl die Frequenz als auch die Antennenkonstruktion bestimmen die erzielbare, maximale Reichweite. Es sollte immer diejenige Kombination aus Frequenz und Antenne gewählt werden, deren resultierender Reichweitenbereich zwar gut für den Anwendungszweck ausreicht, aber nicht deutlich darüber hinausgeht.

Abhängig von Anwendungszweck ist auch die benötigte Speicherkapazität des Transponders ein Kriterium. Ausschlaggebend ist hier das gewählte Datenmodell. Anwendungen nach dem »data-on-network«-Prinzip legen alle ein Objekt betreffenden Informationen in einer (online zugängigen) Datenbank ab und nutzen den RFID-Transponder ausschließlich zur Identifikation. Hier genügt deshalb eine geringe Speicherkapazität von z. B. 96 Bit zur Speicherung einer weltweit eineindeutigen Nummer. Allerdings hat diese Nummer ohne Datenbank-Zugriff keine Bedeutung, was dezentrale Architekturen erschwert. Demgegenüber werden bei »data-on-tag« alle benötigten Informationen direkt auf dem Transponder abgelegt; die Daten sind dadurch dezentral verfügbar, d. h. auch bei Ausfall einer etwaigen zentralen Infrastruktur. Doch die benötigten Speicherkapazitäten können schnell das auf dem Markt Verfügbare übersteigen. Zudem muss ein Konzept überlegt werden, was bei einem Defekt des Datenträgers (z. B. durch mechanische Beschädigung) und dem damit einhergehenden Datenverlust geschehen soll. Für die Praxis empfiehlt sich deshalb eine Mischung beider Konzepte: Einerseits werden die wichtigsten Daten direkt auf dem Transponder mitgeliefert, andererseits aber auch in einer Datenbank gespeichert und um weitere Informationen ergänzt.

Weitere technische Möglichkeiten – entscheidend für die Auswahl der RFID-Produkte – resultieren aus dem Zusammenwirken der Komponenten als Gesamtsystem. Am wichtigsten ist hier die sog. Pulkfähigkeit, d. h. die Möglichkeit, mehrere Transponder gleichzeitig zu erfassen. Sie ist auch ein wichtiger Vorteil von RFID gegenüber Barcodes, weil die Codes nicht vereinzelt werden müssen. So kann z. B. bei einem Wareneingang eine eingehende Sendung in einem Arbeitsschritt komplett registriert werden. Weitere Funktionen betreffen die Datensicherheit der Transponder, wenn z. B. Passwörter oder höherwertige kryptographische Verfahren zum Schutz der gespeicherten Informationen

eingesetzt werden. Auch die Ortung von Transpondern kann eine gewünschte Eigenschaft sein (wenngleich diese in der Regel nur über spezielle Systeme erreicht wird).

Schließlich spielt der Preis eine wichtige Rolle, vor allem bei Anwendungen, die eine sehr große Menge an Transpondern benötigen (z. B. Logistik). Smart Labels sind einfache Transponder, die wie ein Papier- oder Folienetikett auf einen Artikel aufgeklebt werden. Die Kosten sind gering, dafür sind diese Transponder nicht besonders widerstandsfähig. RFID-Transponder, die dauerhaft eingesetzt werden (z. B. Benutzerausweise), sollten deshalb über ein ausreichend robustes Gehäuse verfügen, das die Funktion auch über mehrere Einsatzjahre sicherstellt – auch wenn die Transponder teuerer sind.

Der Frequenzdschungel

In Deutschland wurde der Wert von Funkfrequenzen im Jahr 2000 schlagartig deutlich, als die Auktion der UMTS-Lizenzen über 50 Milliarden Euro in die Staatskasse spülte. Funkfrequenzen sind ein rares Gut, weil zahllose Anwendungen um die Nutzungsrechte konkurrieren: von Polizeifunk über Radio und Fernsehen bis zu Babyphone und Funkfernbedienung für die Auto-Zentralverriegelung.

RFID-Systeme können deshalb nicht beliebig auf eine optimale Frequenz und Kanalbreite setzen, sondern müssen das nutzen, was von den staatlichen Regulierungsbehörden zugeteilt wird. Praktisch ergibt das eine Vielzahl von schmalen Frequenzbändern (Abbildung 1). Im Niederfrequenz (Low Frequency, LF)-Bereich werden 125 KHz genutzt, z. B. zur Tieridentifikation. Größere Bedeutung hat das Hochfrequenz-Spektrum (HF) um 13,56 MHz, das gute Erfassungsraten ermöglicht, gleichzeitig aber einen vergleichweise einfachen Aufbau von Antennen, Transpondern und Lesegeräten zulässt. RFID-Systeme auf HF-Basis sind heute weit verbreitet, weil sie vergleichsweise robust funktionieren und einfach eingesetzt werden können.

Seit einigen Jahren sind auch Ultrahochfrequenzen (UHF) im Einsatz, die in Deutschland das Band 865-868 MHz nutzen. Dieses Frequenzspektrum wurde vor allem durch die Maßnahmen des Handels zur Einführung von RFID bekannt. UHF erlaubt vergleichsweise große Reichweiten bei preisgünstigen Datenträgern. Schließlich gibt es auch Geräte im Mikrowellenbereich, z. B. bei 2,45 GHz. Da derartige Systeme aber aktive Transponder benötigen, sind sie eher für Spezialanwendungen im Einsatz.

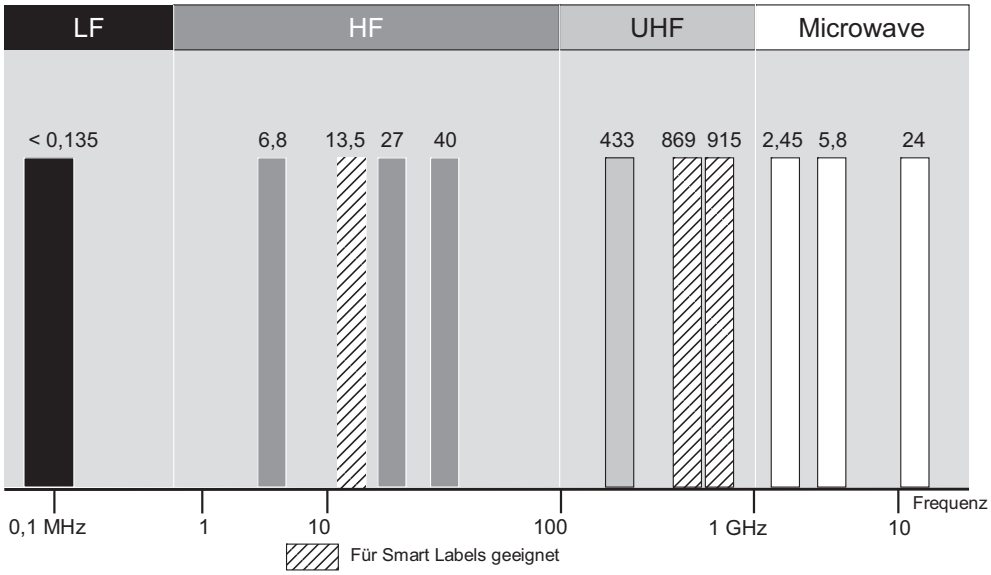


Abb. 1: Für RFID eingesetzte Funkfrequenzen

Damit RFID-Komponenten zueinander kompatibel sind müssen mehrere Voraussetzungen erfüllt sein. Ein RFID-System, das das UHF-Band um 865 MHz nutzt, kann keine Transponder lesen, die für HF ausgelegt sind. Damit nicht genug: Auch das verwendete Datenprotokoll auf der »Luftschnittstelle« muss kompatibel sein. Im UHF-Bereich ist das vergleichsweise einfach, weil sich hier der EPCglobal-Standard »EPC Class 1 Gen-2« durchgesetzt hat und inzwischen auch als ISO-Norm 18000-6C geführt wird. Diese Norm spielt eine erhebliche Rolle bei heutigen und vor allem künftigen RFID-Anwendungen in Logistik und Handel. Die in der Anfangszeit von UHF ebenfalls angebotenen Protokolle ISO 18000-6A und -6B spielen hier kaum noch eine Rolle.

Im HF-Bereich gibt es zwei dominante Standards. Die ISO-Norm 14443 ist vor allem im Bereich Zugangskontrolle, drahtlose Ausweiskarten und Bezahlsysteme eine gewichtige Rolle. Daneben gilt der Standard ISO 15693/18000-3, der sich hauptsächlich für Identifikationsaufgaben in Industrie und Logistik etabliert hat. Beide Standards nutzen zwar die gleiche Frequenz, sind aber nicht zueinander kompatibel.

Technische Grundlagen

HF-Systeme (13,56 MHz)

Bei Systemen auf HF-Basis wird eine induktive Kopplung zwischen Transpondern und Antennen realisiert. Beide Komponenten verfügen über Spulen, über die Spannungen wie bei einem Transformator übertragen werden können. Abbildung 2 erläutert das Grundprinzip. Der Sender treibt einen Strom durch die Spule der Antenne (in der Abbildung links) und erzeugt so ein Magnetfeld. Durch Induktion wird auf der Empfängerseite (Transponder, rechts) eine Spannung erzeugt, die zum Betrieb des Transponder-Chips

genutzt werden kann. Die Datenübertragung erfolgt durch die sog. Lastmodulation: Je nach Information (binäre 0 oder 1) wird ein Lastwiderstand aufgeschaltet, der zu einem geringfügigen Spannungseinbruch an der Sendespule führt. Diesen kann das Lesegerät auswerten.

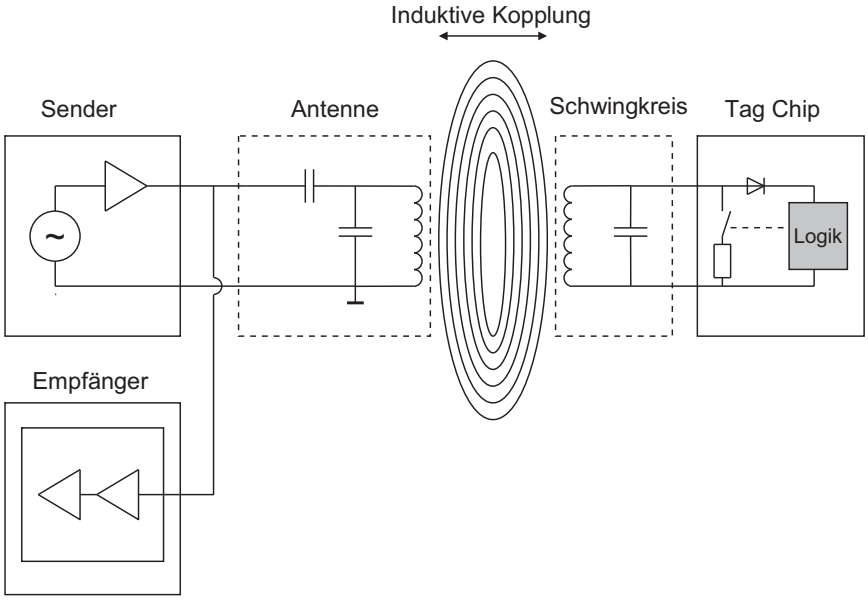


Abb. 2: Aufbau eines HF-RFID-Systems

Durch die Nutzung der induktiven Kopplung bieten HF-RFID-Systeme ein vergleichsweise gut definiertes Übertragungsfeld, das mit zunehmender Entfernung rasch abfällt. Das erfordert zwar auf der einen Seite größere Antennen, wenn größere Reichweiten erzielt werden sollen. Auf der anderen Seite werden durch das begrenzte Lesefeld etwaige Überreichweiten wirksam vermieden. Die charakteristische Spulenform ist bei Transpondern in Smart-Label-Ausführung (d. h. als Etiketten auf Folie oder Papier) gut erkennbar (Abb. 3), wenngleich es die HF-Transponder auch in zahlreichen anderen Bauformen auf dem Markt gibt.

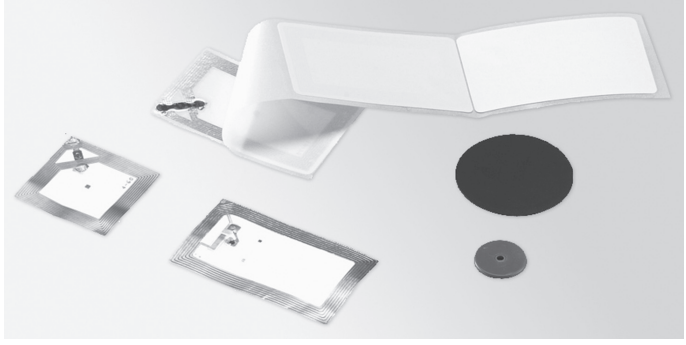


Abb. 3: Typische Bauformen von HF-Transpondern: Links und hinten sog. Smart Labels, rechts Transponder in robustem Gehäuse (Foto: Siemens)

Die wichtigsten Kenndaten von HF-Systemen sind:
- Reichweite: typisch 50-80 cm, max. 1,5 m (allerdings mit erheblichem Aufwand bei der Antennenkonstruktion)
- Speicherkapazität: 12 Byte – 144 KByte
- Pulkfähigkeit: 60 – 200 Transponder (gemäß ISO 15693)

Bei HF-Systemen sind zudem spezielle Erweiterungen möglich. So nutzen drahtlose Smart Cards, die ein hohes Sicherheitsniveau bieten, meist ebenfalls die Frequenz von 13,56 MHz.

UHF-Systeme (865 MHz)

Mit dem Aufkommen der RFID-Anwendungen in Logistik und Handel hat sich auch die Nutzung des UHF-Bandes stark erhöht. Allerdings ist die Frequenz nicht weltweit einheitlich nutzbar: das Spektrum reicht von 865 MHz in Europa über 928 MHz in den USA bis hin zu etwa 950 MHz in Japan. Anwender müssen sich darüber jedoch in der Regel keine Gedanken machen, denn die Transponder sind inzwischen so breitbandig ausgelegt, dass sie in allen Regionen gut funktionieren.

UHF-Systeme nutzen eine echte elektromagnetische Kopplung zwischen Transponder und Erfassungsantenne, d. h. neben der magnetischen Feldkomponente wird auch das elektrische Feld genutzt (Abb. 4). Die Sendeleistung von 2 Watt in Europa erlaubt Reichweiten von 5 m und mehr. Der Transponder verfügt in der Regel über eine mehr oder weniger ausgeprägte Dipolantenne, die die Welle einkoppelt und nach Gleichrichtung dem RFID-Chip zur Verfügung stellt. Die Energieausbeutung ist vergleichsweise gering, so dass nur vergleichsweise einfache Schaltungen mit Strom versorgt werden können – dementsprechend klein ist die mögliche Speicherkapazität. Der Chip antwortet durch eine datenabhängige Reflektion des Sendesignals (backscattering).

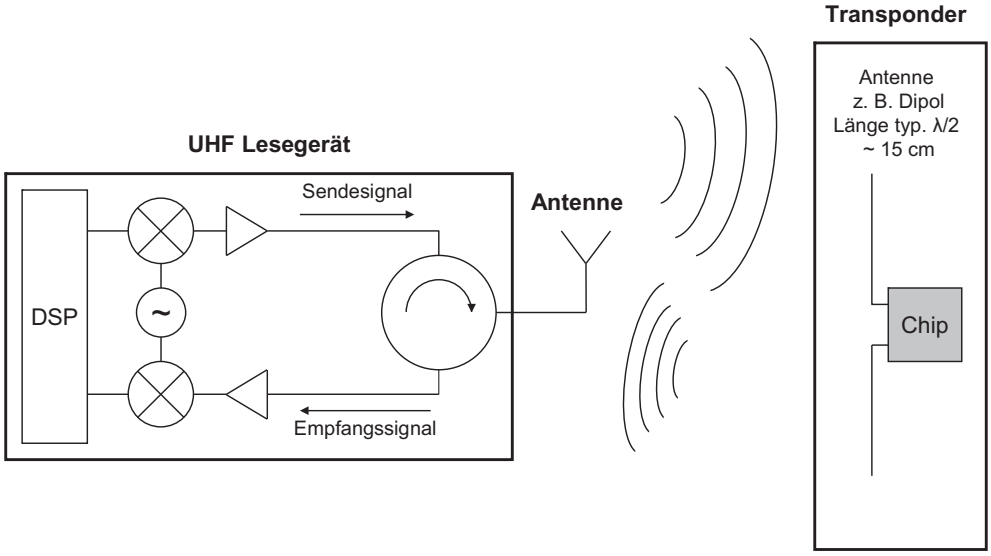


Abb. 4: Aufbau eines UHF-RFID-Systems

Die Nutzung der elektromagnetischen Kopplung bietet einen großen Vorteil: Die erzielbaren Reichweiten sind erheblich höher als bei HF-Systemen, bei gleichzeitig kleineren Antennen-Abmessungen; typische RFID-Universalantennen für UHF haben Abmessungen um 35 x 35 cm. Die größere Reichweite kann allerdings auch ein großer Nachteil sein, da Überreichweiten oft nicht ohne weitere Maßnahmen (z. B. Abschirmungen, Software-Algorithmen) zu vermeiden sind. Ein weiterer Nachteil ist das durch Reflektionen weniger homogene Feld, das zu »Aussetzern« bei der Kommunikation führen kann. Der Effekt ist ähnlich zum Autoradio, das im Stau plötzlich einen schlechteren Empfang hat als noch wenige Meter vorher. Auch haben Flüssigkeiten und metallische Untergründe einen starken Einfluss auf die Erfassungsqualität (eine *Abschirmung* verhindert bei HF und UHF gleichermaßen das Auslesen der Chips). Spezielle Transpondertypen eignen sich jedoch für den Einsatz direkt auf Metall.

Allerdings gibt es auch im UHF-Bereich inzwischen Transponder, die überwiegend induktiv (wie bei HF) angesprochen werden. Mit einer auf die magnetische Feldkomponente optimierten Sendeantenne und einem entsprechenden Transponder-Design ist eine Naherfassung ohne Überreichweiten möglich. Werden diese Transponder mit einer sogenannten Hybrid-Antenne ausgestattet, können sie auch weiterhin im Fernbereich über eine »normale« UHF-Antenne gelesen werden.

Die Antennengeometrien bei den UHF-Smart Labels unterscheiden sich von Typ zu Typ ganz erheblich (Abb. 5); je nach Einsatzzweck werden die Transponder dadurch auf spezielle Eigenschaften optimiert (z. B. Größe, Reichweite). Wie bei HF gibt es auch bei UHF Transponder mit robusten Gehäusen für den Dauerbetrieb in zahlreichen Anwendungsszenarien. Einem Transponder mit festem Gehäuse (z. B. laminiert als Scheckkarte) kann deshalb nicht angesehen werden kann, auf welcher Frequenz der Chip operiert.

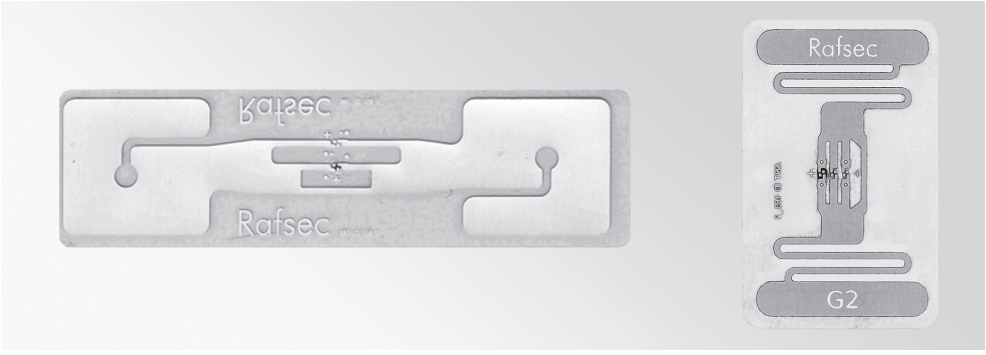


Abb. 5: Beispiele für UHF-Transponder (Foto: Siemens)

Die wichtigsten Kenndaten für UHF-RFID-Systeme lauten:
- Reichweiten bis etwa 5-8 m
- Speicherkapazität: bis 512 Bit
- Pulkfähigkeit: mehrere hundert Transponder

Da aber die UHF-Systeme noch vergleichsweise neu auf dem Markt sind, können für die Zukunft weitere, wichtige Verbesserungen der technischen Daten erwartet werden.

Welches System ist das Richtige?

Eine generelle Empfehlung kann kaum ausgesprochen werden, da zu viele Parameter in die Entscheidung einfließen müssen. Auch führt der technische Fortschritt vor allem bei UHF zu einer immer breiten Einsetzbarkeit dieser Systeme. Bei der Auswahl können die folgenden Kriterien hilfreich sein:

- Welche Reichweite muss das System bieten? Wie problematisch erweisen sich Überreichweiten?
- Welche Materialien (Metall, leitende Kunststoffe, Flüssigkeiten) befinden sich im Umfeld?
- Welche Speicherkapazität wird benötigt? Ist »data-on-tag« oder »data-on-network« vorteilhafter?
- Wie viel Platz ist für die Antennen vorgesehen? Wo werden die Antennen montiert?
- Werden spezielle Zusatzeigenschaften gewünscht?
- Welche Standards sind durch die Applikation oder durch mögliche Projektpartner vorgegeben? Was kann sich hier künftig entwickeln?

Aus technischer Sicht sind auf beiden Frequenzen heute Systeme verfügbar, die zuverlässig, robust und mit hoher Leistung ihre Aufgaben erfüllen.

Literatur

[1] Finkenzeller, K. (2008). RFID-Handbuch. Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. München: Hanser, 5. Auflage.

[2] Horst, D. (2008). RFID-Technologie. In: Bartneck, N./Klaas, V./Schönherr, H. (Hrsg.): Prozesse optimieren mit RFID und Auto-ID. Grundlagen, Problemlösungen und Anwendungsbeispiele. Erlangen: Publicis, 26-40.

[3] Rankl, W. (2008). Handbuch der Chipkarten. Aufbau – Funktionsweise – Einsatz von Smart Cards. München: Hanser, 5. Auflage.

Elektromagnetische Felder zwischen Lebensnotwendigkeit und Hysterie am Beispiel der RFID-Technologie

Kann die Diskrepanz zwischen öffentlicher Risikoeinschätzung und wissenschaftlich abschätzbarem Risiko bei elektromagnetischen Feldern verringert werden?

Achim Enders

Bei der Entwicklung und Markteinführung neuer Technologien können ungünstige Einflüsse auf den biologischen Organismus nicht prinzipiell und schon gar nicht von vornherein ausgeschlossen werden. Negative historische Beispiele belegen dies in mahnender Weise, wie z. B. der anfangs sehr laxe Umgang mit Röntgenstrahlung im Einzelfall zu entsprechenden Spätschäden führte. Wenn auch mittlerweile generell hohe Anforderungen bei der Zulassung bzw. Markteinführung elektrotechnischer Produkte gelten, kann umgekehrt der Beweis einer absoluten Unschädlichkeit prinzipiell nicht geführt werden. Die Existenz von etwas Nichtexistentem kann schon rein logisch nicht beweisbar sein. Die einzig seriöse Fragestellung ist die, wie eine entsprechende Risikoabschätzung aufgrund des wissenschaftlichen Kenntnisstandes und der Datenlage ausfällt, insbesondere, ob es hier noch relevante Unsicherheiten gibt. Letzteres geht bis in den Bereich der Risikokommunikation hinein, denn wen und was hält eine Gesellschaft überhaupt beim Thema Umgang mit Risiken für relevant? Im Folgenden soll der aktuelle wissenschaftliche Kenntnisstand zur Anwendung der RFID-Technologie erläutert werden, ohne hier auf das Thema Risikokommunikation detailliert einzugehen. Naturgemäß ist die Darstellung stark gekürzt, aber für den interessierten Leser werden vertiefende Referenzen angegeben. Es handelt sich um ein Exzerpt eines entsprechenden bebilderten Vortrags beim RFID-Symposium in der Technische Hochschule Wildau [FH] im Oktober 2009, in dem ergänzende Aspekte zur Risikowahrnehmung des Menschen zu finden sind [1].

Einleitung: Derzeitiger Kenntnisstand

Heutige RFID-Systeme benutzen entweder magnetische Nahfelder bei Frequenzen im Bereich bis ca. 20 MHz oder oberhalb gestrahlte elektromagnetische Felder bis ca. 1 GHz zum Aufbau einer Kommunikation zwischen einem Tag und einer Auslesestation, wobei diese Felder mit abnehmender Stärke auch in die Umgebung reichen. Die Frequenzen gehören zum sogenannten nichtionisierenden Teil des elektromagnetischen Spektrums, das auch bei vielen weiteren technischen Applikationen mit einem Erfahrungsschatz von grob 100 Jahren verwendet wird (magnetische Nahfelder werden beispielsweise beim Induktionsherd in der Küche benutzt, gestrahlte Felder beim Fernsehen und Rundfunk wie auch beim schnurlosen Telefon).

Man kennt schädliche Auswirkungen dieser Felder, die in Form von Reizwirkungen im Körper bei niedrigeren Frequenzen (ähnlich zu einem Stromschlag bei direkter Stromzufuhr durch Kabelkontakt) und Erhitzungseffekten bei hohen Frequenzen auftreten (letzteres auch als erwünschter Effekt genutzt in der Mikrowelle). Seit langem gibt es deshalb entsprechende Grenzwertbestimmungen, die dies mit einem großen Sicherheitsabstand verhindern und zu deren Einhaltung entsprechende Vorkehrungen zu treffen sind (z. B. Sicherheitsabstände um Großsendeanlagen herum). Leider gibt es bzgl. der Allgemeingültigkeit der Grenzwertbestimmungen eine kleine, aber wichtige Ausnahme bei Personen mit medizinischen Implantaten wie Herzschrittmachern. Hier sind Einzelfälle einer Beeinflussung der Implantat-Elektronik zumindest bei schlechter konstruierten Altgeräten bekannt geworden. Der physikalische Grund für eine größere Empfindlichkeit technischer Geräte gegenüber elektromagnetischer Feldbeeinflussung als beim Menschen liegt in der schlichten Tatsache, dass Kabel aus Metall elektrischen Strom mindestens eine Million mal besser leiten als biologisches Gewebe. Deshalb kann ein Kabel auch äußere elektromagnetische Felder viel besser in Strom umwandeln als biologisches Gewebe. Gegebenenfalls sind also bei beruflicher Exposition von Implantatträgern, z. B. eben durch RFID-Systeme bei Bibliotheksmitarbeitern, entsprechende Beratungen und Verhaltensmaßregeln durch die Berufsgenossenschaften oder andere zuständige Institutionen notwendig.

Ansonsten ist bei Einhaltung der Grenzwertbestimmungen nach jetzigem Kenntnisstand die Nutzung der elektromagnetischen Felder als sicher einzustufen.

Wissenschaftliche Zweifel?

Dennoch wird, in Analogie zu zahlreichen Umweltskandalen, gerade in den Medien öfter die Frage aufgegriffen, ob es nicht doch schädliche Beeinflussungen des Menschen geben könnte oder, in Konsequenz daraus, ob die heutigen Grenzwertbestimmungen der Weisheit letzter Schluss seien. Diese Fragen werden meist im Zusammenhang mit der Nutzung des Mobiltelefons (»Machen Handys krank?«) oder des Magnetfeldes der Energieversorgung (»Machen Hochspannungsleitungen krank?«) gestellt. In Analogie könnte damit auch die RFID-Technologie in Verruf geraten, wie viele andere neue und alte Systeme übrigens auch. Was ist hierzu über die Medientauglichkeit solcher Schlagzeilen hinaus (»only bad news are good news«) wissenschaftlich zu sagen?

Besonders kritische Organisationen gegen »Elektrosmog« machen die elektromagnetischen Felder z. B. verantwortlich für das Auftreten eines nahezu universellen Spektrums von Krankheiten – dies ist grundsätzlich unglaubhaft, siehe z. B. die dem Mobilfunk zugeschriebenen Gefahren auf einem Flyer [2]. Auch »Appelle« kritischer Ärztegruppierungen gegen den flächendeckenden Mobilfunkausbau konnten nicht unwidersprochen bleiben [3]. Dem ist hinzuzufügen, dass es sich bei diesen Gruppierungen trotz ihrer medienwirksamen, angstschürenden Darstellungen um eine nur sehr kleine Zahl Aktiver handelt. Die Historie, die wissenschaftliche Glaubwürdigkeit und auch das entsprechende Verantwortungsbewusstsein (Angstschüren kann auch krank machen!) derartiger Sichtweisen wird sehr gut nachvollziehbar in einem offenen Internet-Forum dokumentiert [4].

Zusammenfassung

Neben dem gesamten Bild experimenteller Befunde (übrigens in einer sehr guten, öffentlich zugänglichen Datenbank abrufbar [5]), das nach Meinung der weit überwiegenden Mehrheit aller Wissenschaftler für die Anwendbarkeit der heutigen Grenzwertbestimmungen spricht, fehlt es im Gegensatz zu den o. a. Wirkungen oberhalb der Grenzwerte für den Bereich unterhalb auch an einem entsprechenden Einwirkungsmodell. D. h. es gibt keine plausible Erklärung, wie hier die nichtionisierenden elektromagnetischen Felder im biologischen Gewebe zu Beeinflussungen führen könnten. Entsprechende weiterführende Informationen sind zu finden z. B. in der Begründung der sogenannten ICNIRP-Grenzwerte, die die Basis für die allermeisten der internationalen und nationalen Bestimmungen darstellen [6]. Das fehlende Wirkmodell ist letztlich auch das entscheidende Argument, bei der Einführung neuer Technologien unter Nutzung der elektromagnetischen Felder von der Unschädlichkeit dieser Felder auszugehen. Anschaulich gesprochen nutzt jedes neue elektrotechnische Gerät die elektromagnetischen Felder auf seine eigene, spezifische Art und Weise (die beschreibenden technisch-wissenschaftlichen Parameter hierbei sind die benutzten Frequenzen, Feldstärken und die entsprechenden zeitlichen Änderungen) – solange die Grenzwerte nicht erreicht werden, gilt der Betrieb aber als prinzipiell sicher. Dies ist bei der RFID-Technologie grundsätzlich nicht anders, und selbst die Diskussion um eine mögliche »Vorsorge« wird sehr kontrovers diskutiert in dem Sinne, ob ein Anlass zur Vorsorge überhaupt gegeben sein kann. In Bezug auf RFID gibt es hierzu eine neuere Dokumentation [7].

Literatur und Internetquellen

[1] http://www.th-wildau.de/fileadmin/dokumente/bibliothek/dokumente/Enders_RFID_Wildau.pdf

[2] Dachverband der Bürger und Initiativen zum Schutz vor Elektrosmog e. V. (2010). Risiko Mobilfunk. http://www.buergerwelle.de/pdf/risikomobilfunk.pdf

[3] Nieden, Anja ; Dietz, Corinna ; Eikmann, Thomas ; Kiefer, Jürgen ; Herr, Caroline E. W. (2009). Physicians appeals on the dangers of mobile communication – what is the evidence? Assessment of public health data. International Journal of Hygiene and Environmental Health, 212, 576-587

[4] Informationszentrum gegen Mobilfunk, Heidrun Schall. (2011). Elektrosmog-Forum des IZgMF. http://www.izgmf.de/scripts/forum/index.php?mode=index

[5] Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen. (2011) EMF – Portal. http://www.emf-portal.de/

[6] International Commission on Non-Ionizing Radiation Protection (ICNIRP). (2011). Richtlinien für die Begrenzung der Exposition durch zeitlich veränderliche elektrische, magnetische und elektromagnetische Felder (bis 300 GHz). http://www.icnirp.de/documents/emfgdlger.pdf

[7] http://www.bag.admin.ch/themen/strahlung/00053/02644/04794/ index.html?lang=de

Datenschutzrechliche Bedenken beim Einsatz von RFID-Technologie aus europäischer Perspektive[1]

Ulrike Verch

Im europaweiten Vergleich gehören die Niederlande und Finnland zu den Ländern, in denen die RFID-Technologie (radio-frequency identification) am weitesten verbreitet ist. Im Jahr 2009 nutzten nach einer Erhebung von EuroStat, dem Statistischen Amt der Europäischen Union (EU), 9 % der niederländischen Unternehmen RFID-Chips, hauptsächlich zur Produkt- und Personenidentifizierung sowie zur Zugangskontrolle. Der entsprechende Vergleichswert für die Bundesrepublik Deutschland liegt bei 4 % und der europäische Durchschnittswert bei 3 %.[2] Im Jahr 2008 wurden weltweit über 2 Mrd. RFID-Etiketten, wie sie in der Logistik, im Gesundheitsbereich oder auch in Reisepässen und Bibliotheken Anwendung finden, verkauft, davon ungefähr ein Drittel innerhalb Europas. Der Marktwert wird auf rund 4 Mrd. Euro geschätzt und die Europäische Kommission geht davon aus, dass er auf über 20 Mrd. Euro innerhalb der nächsten zehn Jahre steigen wird.[3]

Während die in den Jahren 1995 und 2002 erlassenen Datenschutzrichtlinien der EU[4] die RFID-Technologie nicht explizit erfassen, hat sich die Europäische Kommission durch zahlreiche Veröffentlichungen und Initiativen[5] in den vergangenen Jahren mehrfach des Themas angenommen und mit ihren öffentlichen Online-Konsultationen zur Bürgerbeteiligung aufgerufen.[6] Die Ergebnisauswertung von 2190 Antworten der Online-Konsultation aus dem Jahr 2006 ergab, dass innerhalb der europäischen Bevölkerung große Vorbehalte und Ängste gegen die RFID-Technologie in Hinblick auf den Schutz der Privatsphäre bestehen. So gaben 70 % der Befragten an, dass sie angemessene technische Sicherheitsvorkehrungen zum Schutz ihrer Daten erwarten. Fast genauso viele Bürger wünschten sich mehr Informationen, die über die Potentiale und Risiken der neuen Technologie aufklären und 55 % der Bevölkerung sahen einen gesetzlichen Regelungsbedarf für den Einsatz von RFID-Chips.[7]

---

1 Dieser Beitrag fasst den Diskussionsstand im Frühjahr 2010 zusammen. Entwicklungen seit diesem Zeitpunkt konnten leider nicht mehr berücksichtigt werden.

2 Pressemitteilung STAT/10/12 vom 19.01.2010: Informations- und Kommunikationstechnologien E-Commerce machte 12 % des Unternehmensumsatzes im Jahr 2008 in der EU aus.

3 Pressemitteilung (IP/09/740) vom 12.05.2009: Kleine Chips mit großen Möglichkeiten: Neue EU-Empfehlungen sorgen dafür, dass die »Strichcodes des 21. Jahrhunderts« die Privatsphäre nicht verletzen.

4 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

5 Eine Übersicht findet sich unter: http://ec.europa.eu/information_society/policy/rfid/events/past/index_en.htm.

6 Pressemitteilung IP/06/909vom 03.07.2006:Kommission startet öffentliche Konsultation zur Funkfrequenzkennzeichnung (RFID-Technik) und siehe: http://www.rfidconsultation.eu/.

7 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen (KOM(2007) 96.

»Your Voice on RFID«

Begleitend zur öffentlichen Online-Konsultation konnten unterschiedliche europäische Interessens- sowie Verbraucherverbände ihre Stellungnahmen zu RFID bei der EU-Kommission einreichen und veröffentlichen.[8] Darüber hinaus fanden in Brüssel zahlreiche Workshops und Expertenanhörungen zum Thema statt. Die Ergebnisse dieser Konsultationen wurden in einem englischsprachigen Papier mit dem Titel »Your voice on RFID« zusammengefasst.[9] Neben technischen und sicherheitsrelevanten Aspekten wurden insbesondere auch datenschutzrechtliche Bedenken im Zusammenhang mit der RFID-Technologie thematisiert:

> »It seems currently socially unacceptable that citizens would be tracked and traced wherever they go, all the time. If citizens buy and carry products, this could allow indirect tracking and tracing. [...] As a person can be linked to a RFID serial number (e.g., through the tag in his/her clothes), the distinction between personal data and non-personal data could be blurred.« [10]

Anstatt jedoch zu dieser entscheidenden Frage Stellung zu beziehen, ob eindeutig identifizierbare RFID-Chips, die Privatpersonen mit sich führen, rechtlich als personenbezogene Daten einzuordnen sind und damit dem Anwendungsbereich der EU-Datenschutzrichtlinien unterfallen, kommt das Papier zu dem Schluss, dass es noch zu früh sei, um konkrete gesetzgebende Schritte einzuleiten. Statt dessen sollten zunächst die Anwendbarkeit und Eignung bestehender Rechtsvorschriften und die weitere technologische Entwicklung abgewartet sowie die Forschungsförderung in Bezug auf die RFID-Technologie durch die Europäische Union ausgebaut werden.[11]

In Hinblick auf das Recht der informationellen Selbstbestimmung wird des Weiteren ausgeführt, dass Verbraucher verstärkt Informationen und Aufklärung über die Risiken der RFID-Technologie benötigen. Nur so könnten sie selbstbestimmt entscheiden, ob sie RFID-Chips nutzen möchten. Die Bürger sollten freie Wahlmöglichkeiten haben:

> »RFID should be deployed in such a way that the consumer is in control and can either choose to take advantage of the benefits of RFID usage or value the costs higher and prefer to avoid RFID functionality. At the same time, choices should be easy for consumers to exercise: information concerning RFID should be clear, conspicuous and accurate.« [12]

---

8 Alle sog. »Stakeholder Papers« sind online nachzulesen unter: http://www.rfidconsultation.eu/menu/24.

9 »Your voice on RFID: Background document for public consultation on Radio Frequency Identification (RFID). Summary of five workshops. Open for discussion July-September 2006.« Online unter: http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf

10 Eigene Übersetzung der Autorin: Derzeit erscheint es sozial nicht hinnehmbar, dass Bürger aufgespürt und verfolgt werden, wo immer sie hingehen, jederzeit. Wenn Bürger Produkte kaufen und bei sich tragen, könnte dies eine indirekte Aufspürung und Verfolgung ermöglichen. [...] Da eine Person mit einer RFID-Seriennummer in Verbindung gebracht werden kann, könnte die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten verschwimmen.

11 »Your voice on RFID« (siehe oben).

12 Eigene Übersetzung der Autorin: RFID soll in solcher Weise angewandt werden, dass der Verbraucher die Kontrolle hat und entscheiden kann, ob er sich entweder die Vorteile der RFID-Anwendung zunutze macht oder ob er die Risiken höher bewertet und vorzieht, die RFID-Funktionen zu meiden. Gleichzeitig sollten die Wahlmöglichkeiten für die Verbrauchen einfach auszuüben sein: Informationen über RFID sollen klar, eindeutig und genau sein.

Als weitere Maßnahmen werden vorgeschlagen, dass Selbstverpflichtungserklärungen und Musterrichtlinien für den Einsatz der RFID-Technologie erarbeitet werden, die dann wiederum von einem RFID-Ombudsmann überwacht werden könnten. Schließlich findet sich noch die Empfehlung, in Hinblick auf neue RFID-Einsatzfelder datenschutzrechtliche Risikofolgeabschätzungen (*privacy impact assessments*) nach kanadischem Vorbild einzuführen.

Gestützt auf die Ergebnisse der Expertenmeinungen und der Bürgeranhörung hat die EU-Kommission im Jahr 2007 in einer offiziellen Mitteilung angekündigt, dass sie innerhalb der kommenden zwei Jahre konkrete Leitlinien und Verhaltensregeln zum Einsatz von RFID-Chips erarbeiten und Forschungsaktivitäten auf diesem Gebiet fördern werde.[13] Zu diesem Zweck wurde eine RFID-Sachverständigengruppe ins Leben gerufen, um unter Beteiligung von Interessensvertretern den Dialog weiterzuführen, zukünftige europäische Maßnahmen abzustimmen und eine gemeinsame RFID-Strategie zu erarbeiten.[14] Die datenschutzrechtlichen Empfehlungen enden mit der Ankündigung:

> »Auf dieser Basis wird die Kommission analysieren, welche zukünftigen gesetzgebenden Maßnahmen für die Einhaltung des Datenschutzes und die Wahrung der Privatsphäre erforderlich sind.« [15]

Empfehlungen der EU-Kommission

Wie angekündigt hat die EU-Kommission im Mai 2009 ihre »Empfehlungen zur Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen« veröffentlicht.[16] Das Papier enthält konkrete Vorschläge zu sechs verschiedenen Handlungsfeldern.[17] Neben angekündigten Maßnahmen zur Informationssicherheit und RFID-Anwendungen im Einzelhandel sind für öffentliche Einrichtungen insbesondere die Planungen zur Informationsverbesserung und zur erhöhten Transparenz interessant. So möchte die EU-Kommission ein europaweit einheitliches Kennzeichen für RFID-Anwendungen entwickeln, das den Betreiber und eine Anlaufstelle benennt, bei der weitere Angaben u. a. über den Betreiber sowie den Zweck und Umfang der Datenspeicherung erhältlich sind. Zu den notwendigen Informationen, die für die Bürger einfach und klar verständlich sein sollten, zählt die EU-Kommission auch die

---

13 »Ausgehend von den Ergebnissen der europaweiten Konsultation wird die Kommission überdies die Weiterentwicklung der Technologien für einen besseren Schutz der Privatsphäre als Mittel zur Minderung der Datenschutzrisiken unterstützen.«

14 2007/467/EG: Beschluss der Kommission vom 28. Juni 2007 zur Einsetzung der Sachverständigengruppe für Funkfrequenzkennzeichnung (RFID), in: Amtsblatt Nr. L 176 vom 06/07/2007 S. 0025 – 0030.

15 KOM/2007/0096 endg.: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen {SEK(2007) 312}.

16 Empfehlungen der Kommission vom 12. Mai 2009 (2009/387/EG) zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. - In: Amtsblatt Nr. L 122 vom 16/05/2009, S. 0047-0051.

17 1. Datenschutzfolgenabschätzung, 2. Informationssicherheit, 3. Informationen und Transparenz in Bezug auf die RFID-Nutzung, 4. RFID-Anwendungen im Einzelhandel, 5. Sensibilisierungsmaßnahmen, und 6. Forschung und Entwicklung.

sog. Datenschutzfolgeabschätzung, die den Bürger über die Risiken der konkreten RFID-Anwendung aufklärt sowie über Maßnahmen, die er treffen könnte, um diese Risiken zu mindern.

> »Die Ausführlichkeit der Folgeabschätzung sollte den möglichen Datenschutzrisiken, die mit der Anwendung verbunden sind, angemessen sein.«

Jeder Betreiber von RFID-Anwendungen soll nach Auffassung der EU-Kommission zukünftig eine solche Datenschutzfolgeabschätzung vornehmen, die sechs Wochen vor Einführung der Funketiketten der zuständigen nationalen Behörde vorzulegen und in der auch eine technisch und organisatorisch verantwortliche Person zu benennen ist. Ferner werden in dem Papier weitere Sensibilisierungs- und Forschungsmaßnahmen dargelegt und schließlich die EU-Mitgliedstaaten aufgefordert, innerhalb von zwei Jahren aktiv zu werden, um den Kommissionsempfehlungen nachzukommen.

In der Begründung dieser Maßnahmen stellt die EU-Kommission klar, dass nicht nur RFID-Anwendungen betroffen sind, die personenbezogene Daten verarbeiten, sondern auch solche, die lediglich eine indirekte Personenüberwachung ermöglichen, z. B. Gegenstände im Besitz von Personen, die RFID-Tags mit individueller Artikelkennzeichnung aufweisen.

> »Da die RFID-Technik potenziell sowohl allgegenwärtig als auch praktisch unsichtbar ist, muss bei ihrer Einführung den Fragen der Privatsphäre und des Datenschutzes besondere Beachtung geschenkt werden.[...] Die Mitgliedstaaten und alle Beteiligten sollten insbesondere in dieser Anfangsphase der RFID-Einführung weitere Anstrengungen unternehmen, um sicherzustellen, dass RFID-Anwendungen überwacht und die Rechte und Freiheiten des Einzelnen geachtet werden.«

Internet der Dinge

Mit der Veröffentlichung der Kommissionsempfehlungen haben die politischen Debatten über RFID auf europäischer Ebene jedoch noch keinen Abschluss gefunden. Unter dem Stichwort »Internet der Dinge« (»*Internet of Things*« = *IoT*) diskutiert die Europäische Kommission weiter über mögliche gesetzliche Maßnahmen in Hinblick auf die allgegenwärtige Datenverarbeitung, die in den kommenden Jahren voraussichtlich wachsenden Einfluss auf das wirtschaftliche und gesellschaftliche Leben in Europa nehmen wird.

> »Die Aussichten für diese neue Entwicklung des Internets sind so grenzenlos wie die Zahl der Gegenstände unseres Alltagslebens. Allerdings müssen wir sicherstellen, dass die Europäer als Bürger, Unternehmer und Verbraucher die Technologie gestalten und nicht umgekehrt.« [18]

18 Pressemitteilung (IP/09/952) vom 18.6.2009: Wenn Ihre Joghurtbecher mit Ihnen sprechen: Europa bereitet sich auf die Internet-Revolution vor.

Als sog. Internet der Dinge, das auch unter dem Stichwort Ubiquitous Computing oder Ambient Intelligence diskutiert wird, versteht die Europäische Union die zunehmende elektronische Vernetzung von Alltagsgegenständen und anderen Objekten, die sich entweder mit dem Internet oder untereinander verbinden. Der Einsatz von RFID-Technologie wird als Teilaspekt dieser Entwicklung gesehen, von der sich die EU-Kommission sowohl wirtschaftlichen Fortschritt als auch eine verbesserte Lebensqualität für die europäischen Bürger verspricht.[19] Die EU-Kommission geht von einer rasanten technologischen Entwicklung aus, die einerseits beinhaltet, dass die Größe der Tags stetig abnimmt, während andererseits die Anzahl vernetzter Gegenstände stetig ansteigt, und erwartet eine Zunahme vernetzter Alltagsgegenstände um den Faktor 100 bis 1000 in den nächsten 5 bis 15 Jahren.[20] Angesichts des erheblichen Potentials dieses Wachstumsprozesses in wirtschaftlicher und sozialer Hinsicht hält es die EU für unabdingbar, die Entwicklung nicht allein der Macht des privaten Sektors zu überlassen, sondern maßgeblichen Einfluss und Kontrolle durch die öffentliche Hand auszuüben. Zu diesem Zweck hat sie im Herbst 2008 eine weitere öffentliche Online-Konsultation durchgeführt[21] und im Anschluss dazu im Juni vergangenen Jahres einen Aktionsplan (»Internet of Things – An action plan for Europe«) veröffentlicht, in dem sie weitere Schritte und Maßnahmen ankündigt, wie sie die zukünftige Entwicklung des Internets der Dinge gestalten möchte.[22] Umrahmt von allgemeinen politischen Ausführungen werden in diesem Aktionsplan insgesamt 14 konkrete Handlungsfelder benannt, in denen die EU-Kommission Tätigkeitsbedarf sieht. Neben Ankündigungen zu Umweltaspekten, Forschungsaktivitäten, Standardisierungsbemühungen, statistischen Auswertungen und einem verstärkten internationalen Dialog, finden sich auch Aktionsbereiche in Bezug auf RFID und Datenschutz. Zum einen schlägt die EU-Kommission vor, in Zusammenarbeit mit der Europäischen Agentur für Netz- und Informationssicherheit ENISA[23] sicherheitstechnische Maßnahmen zu verfolgen, um die Privatsphäre der Bürger schon bei der Entwicklung technischer Komponenten durch eingebaute Sicherheitsmechanismen ausreichend zu schützen. Auch technische Möglichkeiten, die RFID-Funktionsweisen der Systeme durch die Nutzer individuell zu steuern, werden als ein wesentlicher Schritt der Vertrauensbildung und gesellschaftlichen Akzeptanz benannt. Zum Schutz vor Missbrauch und Wahrung der Privatsphäre beabsichtigt die Europäische Kommission die datenschutzrechtlichen Aspekte des Internets der Dinge durchgängig zu überwachen, indem sie u. a. weiter den Dialog mit unterschiedlichen Interessensvertretern sucht und sich bei Bedarf zusätzliche gesetzgebende Schritte vorbehält. Und schließlich benennt die Kommission als dritten Aktionsbereich »Das Schweigen der Chips«.

---

19 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen- Internet der Dinge: ein Aktionsplan für Europa (KOM/2009/0278 endg.) vom 18.06.2009.

20 IP/09/952 und KOM/2009/0278 endg. (siehe oben).

21 Siehe: http://ec.europa.eu/information_society/policy/rfid/index_en.htm.

22 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Internet der Dinge: ein Aktionsplan für Europa (KOM/2009/0278 endg.) vom 18.06.2009.

23 European Network and Information Security Agency (http://www.enisa.europa.eu/).

»The Commission will launch a debate on technical and legal aspects of the ›right to silence of the chips‹ which has been referred to under different names by different authors and expresses the idea that individuals should be able to disconnect from the networked environment at any time.« [24]

Über den Ausgang dieser Diskussion und die weiteren vorgeschlagenen Maßnahmen wird die EU-Kommission im Jahr 2012 Bericht erstatten.[25] In der Zwischenzeit werden zu den genannten Aktionsbereichen wieder Expertenanhörungen, öffentliche Ausschreibungen und Online-Konsultationen stattfinden, bei denen die Bürger ihre Interessen einbringen können.[26]

Fazit

Die Europäische Union verspricht sich aufgrund potentieller Kostensenkungen und Effizienzsteigerungen bei den vielfältigen Einsatzmöglichkeiten von RFID-Funketiketten in unterschiedlichen gesellschaftlichen Bereichen ein großes Potential für das wirtschaftliche Wachstum in Europa.[27] Um neue Geschäfts- und damit auch Beschäftigungschancen zu ermöglichen, möchte die Brüsseler Kommission den technologischen Fortschritt der Europäer bei der RFID-Technologie durch weitere Anstrengungen und Forschungsaktivitäten ausbauen und mit entsprechenden Fördermitteln unterstützen.[28] Im aktuellen 7. Forschungsrahmenprogramm der Europäischen Kommission, das sich auf die Jahre 2007 bis 2013 erstreckt, ist das höchste Etatvolumen mit einer Summe von über 9 Mrd. Euro für die Erforschung neuer Informations- und Kommunikationstechnologien vorgesehen. Viele beantragte Projekte beschäftigen sich mit dem Thema RFID, sehr viele mit drahtlosen und ubiquitären Infrastrukturen und wenige Projekte mit dem Datenschutz.[29] Daneben gibt es noch viele andere europäischen Fördertöpfe, aus denen sich der Ausbau der RFID-Technologie finanzieren lässt.[30] So wird beispielsweise die neue Medienausleihe mittels RFID-Verbuchung in der Universitätsbibliothek der Humboldt-Universität zu Berlin durch den Europäischen Fonds für Regionale Entwicklung (EFRE) gefördert.[31]

Trotz dieser starken Förderaktivitäten und positiven Grundeinstellung gegenüber RFID lässt die EU-Kommission kritische Töne insbesondere hinsichtlich der Gefahren für den Datenschutz nicht verkennen:

---

24 Offizielle deutsche Übersetzung: »Die Kommission wird eine Debatte über die technischen und rechtlichen Aspekte des ›Rechts auf das Schweigen der Chips‹ anstoßen, auf das verschiedene Autoren unter unterschiedlichen Bezeichnungen hingewiesen haben und bei dem es darum geht, dass der Einzelne in der Lage sein sollte, sich jederzeit von seiner vernetzten Umgebung abzukoppeln.«

25 Pressemitteilung (IP/09/952) vom 18.6.2009: Wenn Ihre Joghurtbecher mit Ihnen sprechen: Europa bereitet sich auf die Internet-Revolution vor.

26 So ist im Juni 2010 in Brüssel eine Expertentagung zu dem Thema geplant, bei der eine »Roadmap for Europe« erarbeitet werden soll, siehe: http://www.eu-ems.com/summary.asp?event_id=55&page_id=342.

27 Empfehlungen der Kommission vom 12. Mai 2009 (2009/387/EG) zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. - In: Amtsblatt Nr. L 122 vom 16/05/2009, S. 0047-0051.

28 MEMO/08/145 vom 05.03.2008: Radio Frequency Identification Devices (RFID): Frequently Asked Questions.

29 Ausführliche Projektinformationen sind über die Forschungsdatenbank CORDIS abrufbar: http://cordis.europa.eu.

30 Beispielsweise das Förderprogramm CIP = Competitiveness and Innovation Framework Programme.

31 http://www.ub.hu-berlin.de/ueber-uns/partnerschaften/rfid-projekt/rfid-projekt .

»RFID-Tags have the potential to link everyday objects into an ›Internet of Things‹ that will greatly enhance economic prosperity and the quality of life. But as with any breakthrough, there is a possible downside – in this case, the implications of RFID for privacy. This is why we need to build a society-wide consensus on the future of RFID, and the need for credible safeguards. Privacy is at the heart of our European model of society.« [32]

Gleichwohl sind neue Datenschutzverordnungen oder Richtlinien zu RFID in Brüssel derzeit nicht geplant und auch auf bundespolitischer Ebene sind keine aktuellen Verlautbarungen über entsprechende gesetzgebende Maßnahmen erkennbar.[33] Es bleibt indes die Frage offen, wie sich die Bundesrepublik Deutschland zu den Empfehlungen der EU-Kommission zur Wahrung der Privatsphäre in RFID-gestützen Anwendungen vom vergangenen Jahr positionieren wird. Sie ist verpflichtet, der EU-Kommission bis zum Mai 2011 mitzuteilen, welche nationalen Maßnahmen eingeleitet wurden, um den Kommissionsempfehlungen zu entsprechen. Die Europäische Union selbst will erst im Jahr 2012 über weitere mögliche Schritte und Maßnahmen entscheiden.[34] Für die nahe Zukunft ist voraussichtlich eine europaweit einheitliche RFID-Kennzeichnung zu erwarten sowie die Pflicht, RFID-Beauftragte zu benennen, auch wenn sich diese Aufgabe unschwer auf die betrieblichen und behördlichen Datenschutzbeauftragten übertragen ließe. Insgesamt betrachtet werden die Informationspflichten im Zusammenhang mit dem Einsatz der Funketiketten vermutlich erheblich ausgeweitet. Eventuell sind damit auch die von der EU-Kommission geforderten Datenschutzfolgenabschätzungen verbunden.

Öffentliche Einrichtungen und Bibliotheken in Deutschland sollten sich auf eine mögliche Kennzeichnung ihrer RFID-Lesegeräte und RFID-Tags und unter Umständen umfassende Informationspflichten einstellen. Fraglich ist, ob auch eine gesetzliche Verpflichtung eingeführt wird, den Bürgern Wahlmöglichkeiten bezüglich der Nutzung von RFID-Services zu gewähren. Dies würde für Bibliotheken beispielsweise bedeuten, dass sie parallel zur RFID-Medienverbuchung alternative Ausleihmethoden vorhalten und anbieten müssten. Von Seiten der EU gibt es hierzu keine konkrete Empfehlung, jedoch wird im Zusammenhang mit dem RFID-Einsatz im Einzelhandel regelmäßig betont, dass die Verbraucher selbstbestimmt über die RFID-Nutzung entscheiden können, und die Kommission plädiert in ihren Empfehlungen für das sog. Opt-In-Modell, bei dem die RFID-Tags automatisch entfernt werden müssen, es sei denn, der Kunde widerspricht

32 MEMO/08/145 vom 05.03.2008: Radio Frequency Identification Devices (RFID): Frequently Asked Questions. Eigene Übersetzung der Autorin: RFID-Etiketten haben das Potential, Alltagsgegenstände mit dem »Internet der Dinge« zu verlinken, das den wirtschaftlichen Wohlstand und die Lebensqualität erheblich steigern wird. Gleichwohl, wie bei jedem Durchbruch, gibt es auch eine mögliche Kehrseite – in diesem Fall die Auswirkungen von RFID auf die Privatsphäre. Das ist der Grund, weshalb es notwendig ist, dass wir einen gesellschaftsweiten Konsens für die Zukunft von RFID benötigen sowie verlässliche Schutzmaßnahmen. Die Gewährleistung der Privatsphäre ist das Herz unseres europäischen Gesellschaftsmodells.

33 Die letzte ausführliche Stellungnahme der Bundesregierung zu Datenschutzaspekten bei RFID-Anwendungen datiert vom Januar 2008 und beinhaltet einen Verzicht eines gesetzgeberischen Tätigwerdens und empfiehlt die Selbstregulierung des Marktes in Form effektiver Selbstverpflichtungen; vgl. Drucksache 16/7891 vom 23.01.2008: Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie.

34 So zumindest ist der Zeitplan in den Empfehlungen der EU-Kommission festgehalten: Empfehlungen der Kommission vom 12. Mai 2009 (2009/387/EG) zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. - In: Amtsblatt Nr. L 122 vom 16/05/2009, S. 0047-0051.

der Deaktivierung ausdrücklich.[35] Da es bei Bibliotheksbüchern im Gegensatz zum Warenkauf nicht möglich ist, die Funketiketten einfach zu entfernen und die Bibliotheken als öffentliche Einrichtungen darüber hinaus für die Bevölkerung einen wichtigen Versorgungsauftrag haben, auf den viele Bürger angewiesen sind, ließe sich das aktuell diskutierte »Recht auf das Schweigen der Chips« in Bibliotheken am effektivsten durch das Angebot alternativer Ausleihmethoden realisieren.

In mehreren Papieren der EU ist nachzulesen, dass nicht nur RFID-Anwendungen, die sich auf bestimmte oder bestimmbare Personen beziehen, eine Gefahr für die Privatsphäre darstellen, sondern auch Objekte mit einer RFID-Artikelnummer, die sich im Besitz der Bürger befinden und eine indirekte Überwachung erlauben. Für diese sog. potentiell personenbeziehbaren Daten unterliegen die Betreiber bisher nicht den strengen datenschutzrechtlichen Regelungen, obgleich die luxemburgische EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft[36] Viviane Reding hier durchaus einen Regelungsbedarf erkennt:

> »While smart chips working with RFID technology can make businesses more efficient and better organised, I am convinced they will only be welcomed in Europe if they are used by the consumers and not on the consumers. No European should carry a chip in one of their possessions without being informed precisely what they are used for, with the choice of removing or switching it off at any time. The ›Internet of Things‹ will only work if it is accepted by the people.« 37

35 »In addition, to guarantee consumer choice and control, RFID tags that contain personal data should be automatically deactivated at the ›point of sale‹, unless the consumer decides otherwise.« Allerdings sehen die Empfehlungen auch Ausnahmen für den Fall vor, dass die zuvor durchgeführte Datenschutzfolgeabschätzung im konkreten Fall keine Gefahren für die Privatsphäre ergeben haben.

36 Im Jahr 2009 als EU-Kommissarin noch zuständig für die Informationsgesellschaft und Medien.

37 Offizielle Übersetzung: »RFID-Chips können zwar die Effizienz in Unternehmen steigern und ihre Organisation verbessern, doch ist ihre Akzeptanz in Europa nach meiner Überzeugung nur dann gewährleistet, wenn sie von den Verbrauchern und nicht gegen sie verwendet werden. Kein Europäer sollte einen Chip in seinen Sachen mit sich führen, ohne genau darüber informiert zu sein, wozu dieser verwendet wird, und ohne ihn jederzeit entfernen oder ausschalten zu können. Das ›Internet der Dinge‹ wird nur dann funktionieren, wenn es von den Menschen akzeptiert wird« (EU-Kommissarin Reding: Datenschutz der Bürger muss im digitalen Zeitalter Priorität haben (IP/09/571) vom 14.04.2009 und MEMO/09/232.

Literatur und Internetquellen

[1] Pressemitteilung STAT/10/12 vom 19.01.2010: Informations- und Kommunikationstechnologien E-Commerce machte 12 % des Unternehmensumsatzes im Jahr 2008 in der EU aus.

[2] Pressemitteilung (IP/09/740) vom 12.05.2009: Kleine Chips mit großen Möglichkeiten: Neue EU-Empfehlungen sorgen dafür, dass die »Strichcodes des 21. Jahrhunderts« die Privatsphäre nicht verletzen.

[3] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

[4] Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

[5] Pressemitteilung IP/06/909 vom 03.07.2006:Kommission startet öffentliche Konsultation zur Funkfrequenzkennzeichnung (RFID-Technik) http://www.rfidconsultation.eu/.

[7] Stakeholder Papers. http://www.rfidconsultation.eu/menu/24

[8] Your voice on RFID: Background document for public consultation on Radio Frequency Identification (RFID). Summary of five workshops. Open for discussion July-September 2006. http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf

[9] 2007/467/EG: Beschluss der Kommission vom 28. Juni 2007 zur Einsetzung der Sachverständigengruppe für Funkfrequenzkennzeichnung (RFID), In: Amtsblatt Nr. L 176 vom 06/07/2007 S. 0025-0030

[10] Empfehlungen der Kommission vom 12. Mai 2009 (2009/387/EG) zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. – In: Amtsblatt Nr. L 122 vom 16/05/2009, S. 0047-0051

[11] Pressemitteilung (IP/09/952) vom 18.6.2009: Wenn Ihre Joghurtbecher mit Ihnen sprechen: Europa bereitet sich auf die Internet-Revolution vor

[12] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen- Internet der Dinge: ein Aktionsplan für Europa (KOM/2009/0278 endg.) vom 18.06.2009

[13] European Network and Information Security Agency http://www.enisa.europa.eu/.

[14] European Commission Directorate-General Information Society and Media Network Enterprise and RFID, http://ec.europa.eu/information_society/policy/rfid/events/past/index_en.htm

[15] Universitätsbibliothek der Humboldt-Universität zu Berlin. http://www.ub.hu-berlin.de/ueber-uns/partnerschaften/rfid-projekt/rfid-projekt

[16] Drucksache 16/7891 vom 23.01.2008: Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie.

Die zitierten Internetquellen wurden zuletzt am 12.08.2011 aufgerufen.

Bauphysik und bauliche Maßnahmen

Daniel Büth, Wolfgang Meißner

Die RFID-Technologie ist eine bereits seit vielen Jahren genutzte Technologie, welche in einer Vielzahl von Anwendungen fester Bestandteil unterschiedlicher Prozesse ist. Grundsätzlich arbeiten RFID-Geräte auf dem aktuellen Stand der Technik bei fachgerechter Installation zuverlässig und störsicher. Trotzdem sind dies Funkanlagen, welche durch andere Sender, wechselnde Umgebungsbedingungen oder andere Störquellen beeinflusst werden können. Aus den Erfahrungen, welche in weit über 3000 verschiedenen Installationen in unterschiedlichen Bibliotheken und einer Vielzahl von Installationen in anderen Branchen gesammelt wurden, lassen sich verschiedene Richtlinien für die Installation von RFID-Systemen ableiten. Die folgenden Kapitel liefern einen Überblick über verschiedene Anwendungen der RFID-Technologie in Bibliotheken und stellen hilfreiche Hinweise zur Vermeidung von Fehlern und Störungen zur Verfügung. Dabei wird ein besonderes Augenmerk auf die Installation von Gates zur Warensicherung gelegt. Diese sind die leistungsstärksten Komponenten einer Installation und damit verbunden auch diejenigen, welche zum Einen selbst sehr störanfällig sind, zum Anderen aber auch mit anderen Geräten interferieren können.

Einleitung

Die RFID-Technik wird bereits seit vielen Jahren erfolgreich in verschiedenen Bereichen von Industrie, Handel, Verkehr und Logistik eingesetzt. Dabei können mit Hilfe der Transponder und Lesegeräte verschiedene Prozesse zuverlässiger gestaltet und optimiert werden.

Auch im Bereich von Bibliotheken hat sich die RFID-Technik weitgehend durchgesetzt. Hier ergeben sich eine Vielzahl verschiedener Vorteile für Besucher und Betreiber der Bibliotheken. So ermöglicht die RFID-Technologie beispielsweise eine einfache und bequeme Selbstverbuchung der Medien durch den Besucher selbst. Ebenso kann eine Ausleihe und Rückgabe 24 Stunden, 7 Tage die Woche erfolgen. Durch RFID-Gates an den Ein- und Ausgängen der Bibliothek kann eine Diebstahlsicherung der Medien gewährleistet werden. Verschiedene Prozesse, wie die Sortierung, Katalogisierung oder Inventarisierung können automatisch gestaltet werden, wodurch eine erhebliche Zeit- und Kostenersparnis erzielt werden kann.

Die technischen Prozesse sind weitgehend bekannt und werden ständig verbessert. Dabei profitiert man besonders von der Tatsache, dass mittlerweile RFID-Geräte und Transponder nach dem Standard ISO/IEC 15693 und der Frequenz 13.56MHz weltweit in über 3000 Bibliotheken eingesetzt werden. Trotzdem können verschiedene bauliche Gegebenheiten wie ungünstige Positionierung der Leser und Antennen sowie Störungen die Erkennungseigenschaften beeinflussen.

Nach dem erfolgreichen Einzug der HF-Technologie beginnen nun erste Pilotprojekte mit der Einführung der UHF-Technologie (860-960 MHz) in den Bibliothekssektor. Dabei treten zum Einen ähnliche Problemstellung wie im HF-Bereich auf, zum Anderen sind aber auch vollkommen neue Herausforderungen zu bewältigen.

Im Folgenden wird deshalb eine separate Betrachtung der beiden Frequenzbänder durchgeführt. Dabei sind verschiedenen Leseszenarien, welche in einer Bibliothek Anwendung finden können, einzeln zu berücksichtigen. Mögliche Lesepunkte, welche im Folgenden näher betrachtet werden, sind:
- RFID-Gates zur Artikelsicherung an Ein- und Ausgängen
- Selbstverbuchungsautomaten zur Ausleihe durch den Besucher selbst
- Mitarbeiterplätze
- Rückgabeautomaten
- Automatische Sortieranlagen

Die hier beschriebenen Hinweise sollen helfen, bereits bei der Planung die Position und Ausstattung der Bibliothek mit RFID-Geräten zu optimieren.

HF-Antennen-Gates zur Diebstahlsicherung

RFID-Antennen-Gates werden zur Diebstahlsicherung an allen Ein- und Ausgängen der Bibliotheken installiert. Diese Antennen-Gates können als Einzeldurchgang »Single-Gate« (zwei Antennen), »Double-Gate« (drei Antennen) oder mit mehreren Antennen als »Multiple-Gate« aufgebaut werden.

Gute Leseraten können nur dann erreicht werden, wenn die Antennen im richtigen Abstand zu größeren Metallteilen und möglichen Störquellen wie zum Beispiel Energiekabel im Boden oder Wänden montiert sind.

Typische Fehlerquellen, die zu einem unzuverlässigen Betrieb der Geräte führen können, sind:
- Zu große Durchgangsbreiten der Antennen-Gates
- Geländer, Regale oder Tische mit Metallrahmen in unmittelbarer Nähe der Antennen
- Metallträger oder andere große Metallteile in unmittelbarer Nähe der Antennen (Wänden)
- Gegenseitige Beeinflussung der verschiedenen RFID Installationen
- Energiekabel mit hohen Strömen oder andere magnetische Störer in unmittelbarer Nähe der Antennen

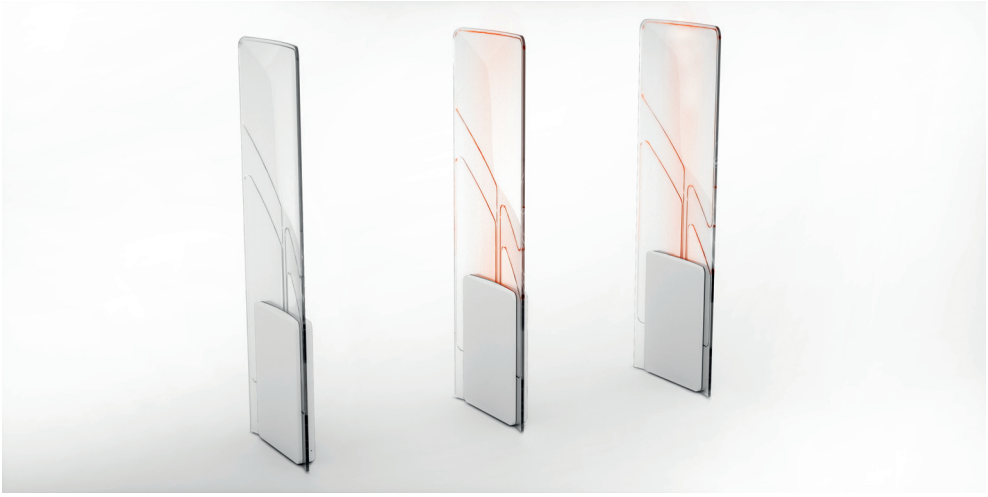


Abb. 1: HF-Crystal-Gate der FEIG ELECTRONIC GmbH mit Alarmleuchte

Viele Antennen besitzen keinen hundertprozentig, dreidimensionalen Erfassungsbereich. Daraus ergeben sich einige Leselöscher im Durchgang in speziellen Ausrichtungen der Transponder. Um ein Höchstmaß an Sicherheit zu gewährleisten, ist es jedoch unabdingbar, dass eine dreidimensionale Erfassung des Transponders innerhalb des Gates möglich ist. Dies bedeutet: unabhängig davon, in welcher Position der Transponder durch das Gate hindurchbewegt wird, auf die komplette Gatebreite gesehen gibt es immer mindestens eine Position in der der Transponder sicher erkannt werden kann. Um eine dreidimensionale Erfassung sicher zu gewährleisten, sollte die lichte Durchgangsbreite zwischen den Antennen 90cm -105cm nicht überschreiten. Kommen Spezialantennen zum Einsatz, so können Durchgangsbreiten von bis zu 130cm realisiert werden. Ist eine eindimensionale Erfassung des Transponders ausreichend, so darf die Durchgangsbreite bis zu 160cm betragen.

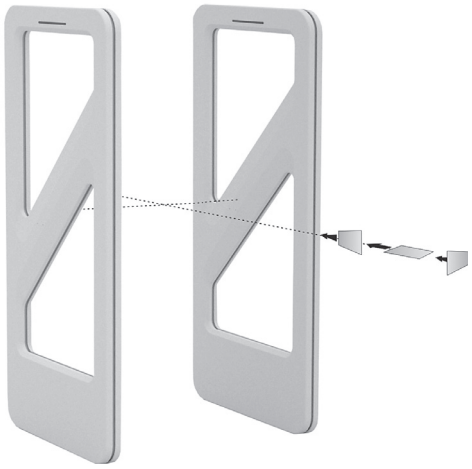


Abb. 2: dreidimensionale Erfassung eines Transponders

Ein weiteres Problem können Metallteile in der Nähe der Antennen darstellen. Dies betrifft beispielsweise Geländer, Regale oder Tische mit Metallrahmen. Ebenso können dies fest installierte Metallteile wie Rolltreppen oder Fahrstühle und baulich bedingte Metallteile wie Stahlträger oder eine Deckenbewehrung sein. Metall und andere leitende Materialien kann ein magnetisches Feld nicht durchdringen. Dadurch werden der Feldlinienverlauf und die Induktivität der Antenne verändert. Dies resultiert in einer starken Beeinflussung des Systems. Weiterhin wird das Feld durch die Gegeninduktivität bzw. die Wirbelströme im Metall geschwächt. Der Einfluss von Metall auf die Performance / Lesereichweite eines RFID-Systems ist in Abbildung 3 zu sehen.

In dem Bild wird von einer Leser-Antennen-Konstellation ausgegangen, welche unter Idealbedingungen eine maximale Lesereichweite von 80cm erzielen kann. Werden Metallteile in die Nähe der Antenne gebracht, so bricht die Leseperformance drastisch ein. Ein größeres Metallteil in 10cm Entfernung von der Antenne bewirkt, dass sich die Lesereichweite halbiert. Bei einer Entfernung von 25cm zwischen Metall und Antenne beträgt die Lesereichweite noch 75 % derer unter Idealbedingungen. Der störende Einfluss von Metall auf die Induktivität einer Antenne kann durch einen erneuten Abgleich der Antennenschleife kompensiert werden. Damit wird die Antenne auf die speziellen Umgebungseinflüsse abgestimmt. Zwar kann damit die Performance des Systems um einiges verbessert werden, jedoch wird es nicht möglich sein den störenden Einfluss von Metall in kurzer Distanz zur Antenne vollständig zu eliminieren. Nach einem erfolgten Antennenabgleich kann ein Transponder über 65cm gelesen werden, wenn sich die störenden Metallteile nur 10cm entfernt von der Antenne befinden. Bei einer Entfernung von 25cm zwischen Antenne und Metall ist nur noch eine geringe Beeinflussung messbar. Hier kann eine Lesung bereits über eine Entfernung von 75cm erfolgen.

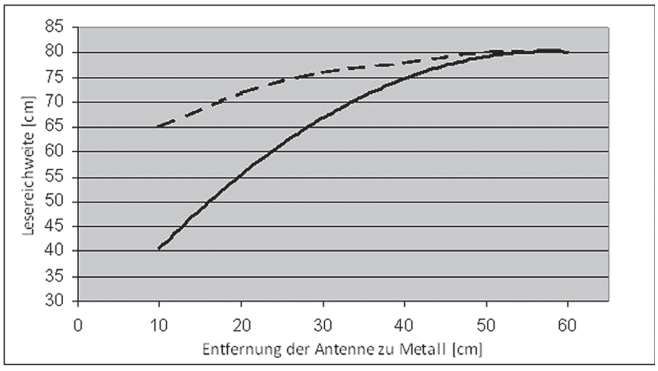


Abb. 3: Einfluss von Metall auf die Performance eines RFID-Systems

Grundsätzlich gilt, dass eine Antenne mindestens in einem Abstand von 50cm zu größeren Metallteilen aufgestellt werden sollte, damit eine Beeinflussung des Leseverhaltens vermieden werden kann. Sind Abweichungen von der bestmöglichen Performance des Systems in der Applikation akzeptabel, so sollte dennoch ein Mindestabstand von 20cm nicht unterschritten werden.

Von entscheidender Bedeutung für die Performance eines RFID-Gates ist auch die gegenseitige Beeinflussung verschiedener RFID-Leser untereinander. Hier gilt es folgende Szenarien zu betrachten:

- Lichter Abstand zweier Antennen mit unabhängigen Lesern zueinander
- Lichter Abstand zweier Antennen mit einem gemeinsamen Leser zueinander
- Lichter Abstand einer Antenne zu Selbstverbuchungsautomaten, Mitarbeiterplätzen, Rückgabestationen und Sortieranlagen

Werden zwei Antennen mit zwei unabhängigen Lesern in einer Applikation betrieben (z. B. getrennter Ein- und Ausgang), so sollte ein lichter Mindestabstand von 8m zwischen beiden Standorten eingehalten werden. Anderenfalls kann es zu einer Interferenz zwischen beiden Systemen kommen, wodurch eine Identifikation von Transpondern nahezu unmöglich wird. Dieser Abstand kann durch zwei verschiedene Maßnahmen bis auf 1m reduziert werden. Hier bietet sich entweder die Möglichkeit beide Leser miteinander zu synchronisieren (Readersynchronisation) oder ein Multiplexen der Leser (Readermultiplexing) durchzuführen. Bei beiden Maßnahmen ist eine zusätzliche Verkabelung erforderlich, welche die beiden Leser miteinander verbindet.

Bei der Readersynchronisation stellt ein erster Leser den Master dar. Zu einem bestimmten Zeitpunkt sendet der Master einen Triggerpuls über die Steuerleitung an die benachbarten Leser. Dieser Puls stellt das Startsignal für die RF-Kommunikation dar. Alle Leser beginnen daraufhin gleichzeitig mit dieser.

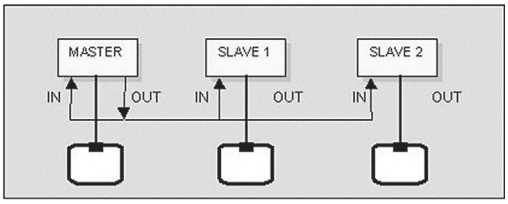


Abb. 4: Prinzip der Readersynchronisation

Im Falle des Readermultiplexings stellt ebenfalls ein erster Leser den Master dar. Dieser ist als erstes berechtigt eine RF-Kommunikation durchzuführen. Hat er diese beendet, so sendet er einen kurzen Puls an einen benachbarten Leser. Daraufhin ist dieser berechtigt eine Kommunikation zu beginnen. Nachdem er diese beendet hat, sendet er wiederum einen Triggerpuls an den nächsten Leser. Beim Readermultiplexing handelt es sich somit um eine Reihenschaltung von Lesern.

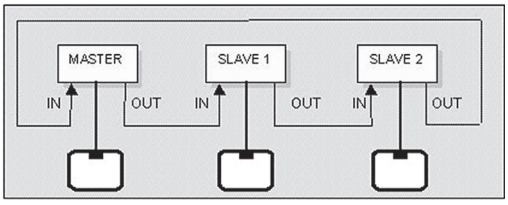


Abb. 5: Prinzip des Readermultiplexing

Werden mehrere Gates von einem Leser aus angesteuert, so ist eine maximale Kabellänge von 6m zulässig. Werden größere Kabellängen benötigt, so sind Performanceverluste mit einzukalkulieren. Bei einer Kabellänge von 11m ist mit etwa 6-10% Leistungsverlusten zu rechnen.

Der Vorteil beim Betrieb mehrerer Antennen an einem Leser besteht darin, dass die Antennen über einen Multiplexer angesteuert werden können. Dies hilft zum Einen die Kosten für Leser zu senken, zum Anderen kann damit auf zusätzliche Synchronisationsmaßnahmen verzichtet werden.

Ebenfalls kann es zu einer Beeinflussung zwischen RFID-Antennen und Selbstverbuchungsautomaten, Mitarbeiterplätzen, Rückgabestationen und Sortieranlagen kommen. Hier gilt zu berücksichtigen, dass durch zusätzliche Abschirmmaßnahmen Mindestabstände erheblich reduziert werden können. Ohne eine Schirmung sollte ein Mindestabstand von 5m zu einem Selbstverbuchungsautomaten nicht unterschritten werden. Mit einer zusätzlichen Schirmung kann dieser auf 2m reduziert werden.

Der Mindestabstand zu Rückgabestationen und Sortieranlagen ist immer abhängig von der Sendeleistung, der Größe der Antenne, sowie der Schirmung. Gewöhnlich ist hier mit einem Abstand zwischen 1m und 10m zu rechnen.

Eine weitere mögliche Fehlerquelle, welche die Performance eines Gates zur Warensicherung erheblich beeinflussen kann, stellt eine unsaubere Spannungsversorgung dar. Dies kann beispielsweise durch andere elektronische Geräte hervorgerufen werden, welche am gleichen Stromkreis angeschlossen sind. Hier ist es ratsam einen eigenen Stromkreis für den Betrieb der Gates vorzusehen. Falls dennoch weitere Störungen in der Spannungsversorgung auftreten, kann ein zusätzlicher EMV Filter vorgeschaltet werden.

Problematisch sind ebenfalls Energiekabel, Computermonitore und große Leuchtstoffröhren, welche in der Nähe der Antennen verlaufen oder montiert sind. Zu Energiekabeln ist unbedingt ein Mindestabstand von 1m in alle Richtungen einzuhalten. Bei Computermonitoren (CRT-Röhre) sollte ein Abstand von 60cm eingehalten werden. Zu großen Leuchtstoffröhren und Leuchtreklamen gilt es einen Abstand von 2m einzuhalten.

UHF-Antennen-Gates zur Diebstahlsicherung

Typische Anwendungen für UHF-Antennen-Gates sind auf Grund der großen Lesereichweite, welche mit einem solchen System erzielt werden kann, bisher überwiegend im Bereich der Logistik zu finden. Hier werden UHF-Gates gewöhnlich zur Kontrolle des Wareneingangs und Warenausgangs in Verteilzentren und Märkten verwendet. Diese sind in der Regel recht großzügig und robust konstruiert und daher für einen Einsatz in Bibliotheken, welche hohe Anforderungen an Architektur und Design stellen, nicht geeignet. Dennoch kann von denen im Logistiksektor gewonnenen Erfahrungen in dieser sehr frühen Phase der UHF-Technologie im Bibliothekswesen profitiert werden.

Abb. 6: UHF-Portal im Logistikbereich ©Bühnenbau Schnakenberg GmbH & Co. KG

Im Wesentlichen besteht ein UHF-Gate aus einem Long Range Leser und mehreren Antennen. Diese sind erforderlich um eine lückenlose, dreidimensionale Erfassung innerhalb des Gates sicher zu stellen. Mit nur einer angeschlossenen Antenne kann lediglich eine zweidimensionale Erfassung ermöglicht werden. Die Antennen werden mittels eines Koaxialkabels an den Leser angeschlossen und an beiden Seiten, in den oberen Ecken oder oberhalb des Kontrollpunktes montiert. Auf Grund des begrenzten Öffnungswinkels einer UHF-Antenne (in der Regel ca. 65°) ist dabei zu beachten, dass die gesamte Durchgangsfläche erst in einem bestimmten Abstand zur Antenne abgedeckt werden kann. Zwischen den beiden Antennen treten in kurzer Distanz Leselöcher auf, in denen Transponder nicht erkannt werden können.

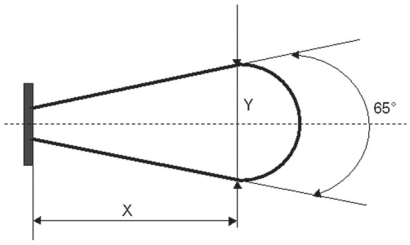


Abb. 7: Öffnungswinkel einer UHF-Antenne

Deshalb ist bei der Planung der Gates an den Ein- und Ausgängen unter allen Umständen zu beachten, dass die Antennen soweit zurückgesetzt montiert werden, dass im Durchgangsbereich eine lückenlose Erfassung möglich ist. Da nicht permanent Personen durch jedes Gate hindurch gehen, empfiehlt es sich die einzelnen Lesestationen zu triggern. Dazu eignen sich Signalgeber jeder Art, wie z. B. Bewegungsmelder oder Lichtschranken. Alle gängigen UHF-Long-Range-Leser verfügen über mindestens einen digitalen Eingang, auf dem Triggersignale empfangen und zur Steuerung des Lesers verwendet werden können.

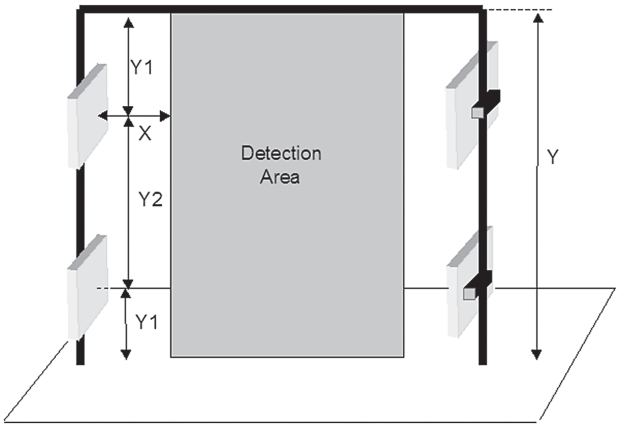


Abb. 8: Typische Anordnung von Antennen in einem UHF-Gate

Der Vorteil der Triggerung besteht dabei darin, dass das RF-Feld des Lesers nur dann eingeschaltet ist, wenn dies unbedingt erforderlich ist. Dies trägt zum Einen dazu bei, den Traffic und mögliche Störungen auf der Luftschnittstelle zu reduzieren, zum Anderen wird durch die Triggerung der Energieverbrauch gesenkt, da im »Standby« die Stromaufnahme des Systems deutlich geringer ist.

Nach dem Standard EN 302208 stehen vier unterschiedliche Sendekanäle mit einer Kanalbandbreite von 200 kHz zur Verfügung. Zwischen den einzelnen Sendekanälen ist ein Schutzband von 600 kHz angesiedelt. Das Kommunikationsverfahren ist so ausgewählt, dass eine beliebige Anzahl von Lesern auf der gleichen Frequenz betrieben werden kann. Dies wird ermöglicht durch die Tatsache, dass die Transponderantwort spektral von den Signalen der Leser getrennt wird und in der Mitte des 600 kHz breiten Schutzbandes angeordnet wird. Dadurch wird eine Überlagerung der Transponderantwort durch andere aktive Leser vermieden.

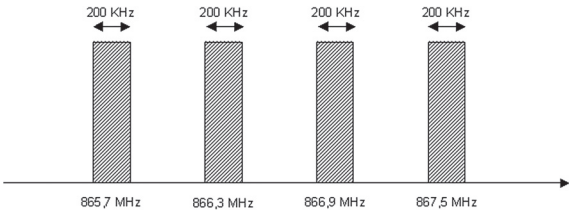


Abb. 9: 4-Kanalplan nach ETSI EN 302208

Ein typisches UHF-Antennenfeld ist in Abb.10 zu sehen. Dabei fällt auf, dass in einem bestimmten Bereich vor der Antenne ein geschlossenes, homogenes Feld existiert, in welchem ein Transponder sicher erkannt werden kann. Mit zunehmendem Abstand von der Antenne treten erste Leselöcher auf, in denen die Feldstärke nicht ausreichend groß ist, um einen Transponder zu aktivieren. Je weiter man sich von der Antenne entfernt, umso größer und zahlreicher werden diese Leselöcher, bis schließlich nur noch einige wenige Bereiche existieren, in denen der Transponder gelesen werden kann.

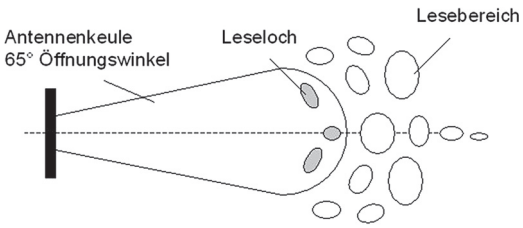


Abb. 10: Typisches UHF-Antennenfeld

Durch Reflektionen kann es sowohl zu einem gehäuften Auftreten von Leselöchern, als auch zu Überreichweiten kommen. Gewöhnlich treten beide Phänomene gleichzeitig auf. Reflexionen entstehen an allen Gegenständen im Bereich eines Gates. Wichtig ist zu beachten, dass durch jede Änderung innerhalb eines UHF-Feldes die Eigenschaften der Applikation verändert werden. Bewegt sich beispielsweise eine Person durch ein Gate, so verändert sich das Feld mit jedem Schritt. Es kommt zu einer ständigen Verschiebung von Leselöchern und Lesebereichen. Kommt es zu einer Überlagerung von Wellen mit um 180° verschobener Phase, so kommt es zur Auslöschung des Signals und es entsteht ein Leseloch. Überlagern sich Wellen mit gleicher Phase, so kommt es zu einer Verstärkung des Signals, so dass erhebliche Überreichweiten erzielt werden können. Besonders begünstigt werden Reflektionen durch Metall. An metallischen Oberflächen entsteht eine Totalreflektion. Neben dieser Eigenschaft können ebenfalls Wellen auf der Oberfläche eines Metalls weitergeleitet werden. Durch die Weiterleitung von Wellen entlang der Oberfläche kann es vorkommen, dass Transponder, welche sich in großer Entfernung zur Antenne befinden, ebenfalls noch detektiert werden. Dabei können Entfernungen von bis zu 50m überbrückt werden. Typischerweise treten solche Phänomene baulich bedingt auf. Die Wellen werden entlang von Stahlträgern oder Rohren (Heizung, Wasser, etc.) weitergeleitet.

Sind zwei benachbarte UHF-Portale zu dicht aneinander installiert, so besteht die Möglichkeit, dass bedingt durch Reflexionen oder die Weiterleitung von Wellen entlang einer metallenen Oberfläche, Transponder in benachbarten Gates ebenfalls erfasst werden und somit keine eindeutige Zuordnung mehr erfolgen kann. Besonders problematisch ist dies, wenn Ein- und Ausgang dicht nebeneinander liegen.

Während bei Anwendungen im HF-Band (13,56 MHz) benachbarte Gates durch geeignete Synchronisationsmaßnahmen störungsfrei parallel betrieben werden können, sind bei Gateanwendungen im UHF-Bereich verschiedene Szenarien zu unterscheiden. Sind zwei Antennen-Gates mit geringer Durchgangsbreite und minimalem Abstand zueinander

installiert, so dass durch die beiden Gates eine maximale Distanz von 5m abgedeckt wird, dann ist zwischen den beiden Portalen unbedingt eine geeignete Schirmung zu installieren. Dies ist erforderlich, da eine Lesung von Transpondern, welche sich in dem benachbarten Durchgang befinden, erfolgen kann. Ebenso ist es möglich, dass es durch die Einkopplung von Signalen in die Antennen des benachbarten Tores zu einer Übersteuerung des Empfängers des Lesers im Nachbartor kommen kann. Ebenso kann dadurch der Transponder empfindlich gestört werden, so dass dieser keine klaren Informationen empfängt und nicht antwortet. Wird mit zwei Portalen eine Strecke von 6 -8m abgedeckt, so ist es von der Position der Antennen abhängig, ob eine zusätzliche Trennung der beiden Tore vorgenommen werden muss. Diese ist dann erforderlich, wenn Antennen parallel zueinander montiert sind und direkt ineinander koppeln können. Wird eine Distanz von mehr als 8m mit den beiden Toren abgedeckt, so kann auf eine zusätzliche Schirmung verzichtet werden, da bedingt durch die Freiraumdämpfung die abgestrahlten Signale so stark gedämpft werden, dass es nicht mehr zu einer Übersteuerung benachbarter Geräte kommen kann.

Als Abschirmmaterialien zur Trennung der beiden Gates eignen sich Metallplatten oder Absorbermatten. Einfache Metallplatten besitzen den Vorteil, dass sie preiswert sind. Allerdings werden durch zusätzliche metallische Gegenstände im Bereich eines Gates die Anzahl der Reflektionen erhöht, durch welche zusätzliche Leselöcher entstehen und die Performance des Gates verringert wird. Eine lückenlose Erfassung im Bereich innerhalb des Gates kann in diesem Fall nicht sicher gewährleistet werden. Diesen Nachteil besitzen spezielle Matten, welche aus einem absorbierenden Material hergestellt werden, nicht. Hier werden nahezu alle auf die Oberfläche auffallenden Wellen absorbiert. Problematisch ist bei diesen allerdings die Tatsache, dass sie sehr kostenintensiv sind, wodurch der Preis für eine Installation schnell ansteigt.

Befinden sich mit einem Transponder versehene Artikel in der Nähe des Gates oder werden mit einem Transponder gekennzeichnete Bücher oder Medien durch eine Person vor dem Gate vorbei bewegt, kann es, bedingt durch Reflektionen und Überreichweiten, gehäuft zu Fehlalarmen kommen. Deshalb sollte beachtet werden, dass in einem Bereich von mindestens 8m vor und hinter dem Gate keine Bücher oder Medien gelagert oder bewegt werden.

Problematisch ist ebenfalls, dass durch die große Reichweite eines UHF-Systems eine Vereinzelung von Personen an Ein- und Ausgängen nahezu unmöglich ist. Dies gestaltet sich dann als problematisch, wenn ein nicht verbuchtes Buch oder Medium in einer größeren Gruppe von Personen durch das Gate getragen wird. Hier kann der Täter nicht eindeutig identifiziert werden und die gesamte Gruppe steht zunächst unter Generalverdacht. Tritt dies entweder durch tatsächlichen Diebstahl oder Fehlalarm gehäuft auf, so könnte dies schnell den Unmut der Besucher nach sich ziehen.

Neben Metall stellen Flüssigkeiten ein weiteres kritisches Element dar. Flüssigkeiten führen zugleich zu Reflektionen und Absorptionen. Wellen werden an der Oberfläche von Flüssigkeiten gebrochen und teilweise reflektiert. Der nicht reflektierte Teil wird von der Flüssigkeit absorbiert. Eine Durchdringung der Flüssigkeit ist nahezu ausgeschlossen.

Dies kann ebenfalls zu Problemen bei der Warensicherung führen. Da der menschliche Körper zu über 70% aus Wasser besteht, ist er hervorragend geeignet Transponder abzudecken. Werden Bücher in der Mitte einer größeren Gruppe von Personen durch ein Gate bewegt oder unter dem Arm getragen, so wird eine erfolgreiche Identifikation deutlich erschwert und je nach Grad der Abdeckung des Transponders sogar unmöglich.

Selbstverbuchungsplätze. Mitarbeiterplätze, Rückgabeautomaten und Sortieranlagen mit HF-Technologie

In modernen Selbstverbuchungseinheiten und Mitarbeiterplätzen werden gewöhnlich Mid-Range-Leser und Antennen in der Größenordnung eines DIN A4 Blattes eingesetzt. Mit einer vom Leser abgegebenen Sendeleistung von 1 Watt und einem typischen Buchtransponder (Größe: 45mm x 76mm) ist eine Lesereichweite von 30 -40cm bei paralleler Labelorientierung zur Antenne möglich.

Abb. 11: Leser und Padantenne für Selbstverbuchungsautomaten und Mitarbeiterplätze

Solche Systeme werden typischerweise in der Nähe von Ein- und Ausgängen montiert. Dadurch können diese Stationen relativ Nahe an die Gates zur Artikelsicherung heranrücken. Um längere Wartezeiten zu vermeiden, werden oftmals mehrere Einheiten nebeneinander aufgestellt. Aus diesem Grunde ist es erforderlich zweierlei Mindestabstände näher zu betrachten.

- Mindestabstand zu Antennen der Gates
- Mindestabstand zu benachbarten Selbstverbuchungsstationen

Zu benachbarten Gate-Antennen sollte der Abstand mindestens 5 -7m betragen. Dies ist abhängig von den verwendeten Antennen. Da die Leser in Selbstverbuchungsplätzen, Rückgabeautomaten oder Mitarbeiterplätzen mit wesentlich geringerer Leistung operieren, als dies bei Gates der Fall ist, sollte lediglich ein Abstand von 2 -3m zwischen zwei benachbarten Stationen eingehalten werden.

Durch zusätzliche Abschirmmaßnahmen können die angegebenen Mindestabstände weiter reduziert werden. Einen positiven Nebeneffekt stellt die Tatsache dar, dass hierdurch ungewollte Lesungen von Transpondern im Bereich außerhalb der Antenne verringert werden. Prinzipiell sind zwei unterschiedliche Ausführungen der Schirmung denkbar.

– Abschirmung der Antenne an 5 Seiten mit Hilfe einer Wanne aus Metall.
– Einschränkung des Erfassungsbereichs durch eine flach aufliegende Metallplatte mit Antennenaussparung.

Die Abschirmung der Antenne mit einer Wanne kann aus Metallblech oder Metallfolie hergestellt werden. Dabei sollte die Wanne so ausgelegt werden, dass parallel zur Antennenfläche ein Mindestabstand von 10cm gewährleistet ist. Der seitliche Abstand der Wanne zur Antenne sollte mindestens 6cm betragen.

Die Metallplatte zur Einschränkung des Erfassungsbereichs sollte am Rande der Antenne verlaufen. Der seitliche Mindestabstand der Schirmung zur Antenne sollte 2 -3cm betragen.

In RFID-Rückgabeautomaten sind oft Antennen der Größe 20cm x 20cm bis 30cm x 30cm installiert. Die Medien liegen hier horizontal im Automaten. Dadurch ergibt sich in der Regel eine eindimensionale Erfassung. Oft befinden sind diese Automaten in einem geschlossen Metallgehäuse. Hier ist es besonders wichtig die notwendige Reichweite und Lesegeschwindigkeit zu kennen, damit das System passend ausgelegt werden kann und der störende Einfluss des Metalls eine erfolgreiche Umsetzung des Szenarios nicht verhindert.

Auch in Sortieranlagen liegen die Bücher/Medien oft auf einem Förderband oder anderen kleinen Transportanlagen. Hier ist ebenfalls nur eine eindimensionale Erfassung erforderlich.

Typische Probleme, welche in Bezug auf Rückgabeautomaten oder Sortieranlagen auftreten können, sind:
– Störungen in der Antenne
– Unzureichende Lesereichweite der Medien (CD, DVD,...)
– Zu geringe Lesegeschwindigkeit des RFID-Systems

Um die Beeinflussung des Systems so gering wie eben möglich zu gestalten sollten verschiedene Maßnahmen ergriffen werden. So sollten beispielsweise benachbarte Sortieranlagen und Rückgabeautomaten in einen Mindestabstand von ca. 2 -3 m zueinander montiert werden. Die Rahmen der Anlagen sollten elektrisch isoliert sein. Gegebenenfalls sollte eine Isolation (Kunststofffolie) zwischen den Rahmen vorgesehen werden. Die Antennen selbst sollten mit einem Mindestabstand zu Metall von 10cm montiert werden. Zu Gates sollte ein Mindestabstand von 8m eingehalten werden.

Selbstverbuchungsplätze. Mitarbeiterplätze, Rückgabeautomaten und Sortieranlagen mit UHF-Technologie

Wie in klassischen HF-Anwendungen werden auch im UHF-Bereich an modernen Selbstverbuchungsplätzen und Mitarbeiterplätzen Lesereichweiten von maximal 30 -40 cm benötigt. Diese können mit einem UHF-System relativ mühelos erzielt werden. Dafür eignen sich beispielsweise kleine Lesermodule, welche frei verbaut werden können oder

fertige Desktopleser mit integrierter Antenne, welche mühelos per USB an einen PC angeschlossen werden können.

Abb. 12: UHF-Mit-Range Leser mit integrierter Antenne und UHF-Modul mit Desktopantenne

Solche Leser arbeiten gewöhnlich mit einer Leistung von wenigen Milliwatt um die benötigte Lesereichweite zu erzielen. Problematisch gestaltet sich dabei allerdings das Feld der Antenne auf den gewünschten Bereich zu beschränken. Physikalisch bedingt ist das Feld auf Grund der kleinen Bauform der Antennen weniger gerichtet. Reflektionen stellen eine zusätzliche Schwierigkeit dar. Dadurch können ebenfalls Bücher in der näheren Umgebung der Selbstverbuchungsautomaten gelesen werden. Um den Selbstverbucher herum sollten deshalb in einem Abstand von mindestens 2m keine Bücher gelagert werden. Ebenso besteht das Risiko, dass Bücher, die der Kunde noch in seiner Hand hält oder Bücher, welche von wartenden oder vorbeigehenden Kunden mitgeführt werden, ebenfalls gelesen werden und zu falschen Buchungen führen. Hier sollten unbedingt weitere Abschirmmaßnahmen ergriffen werden. Am Selbstverbuchungsautomaten sollte ebenfalls der Bereich, in dem das Buch oder Medium erfasst werden sollte, seitlich und nach oben hin mit einem Absorbermaterial begrenzt werden. Dies trägt dazu bei zusätzliche Reflektionen zu vermeiden und das Lesefeld auf den gewünschten Bereich zu konzentrieren. Der Mindestabstand zwischen zwei benachbarten Arbeitsplätzen oder Selbstverbuchungsautomaten sollte ebenfalls mindestens 2m betragen. Da es sich bei einem UHF-Leser um ein aktives Funksystem handelt, kann es zu einer Beeinflussung anderer elektronischer Geräte kommen. An Mitarbeiterplätzen sind davon speziell Computermonitore betroffen. Hier gilt, dass ein Mindestabstand von 1m eingehalten werden sollte.

Die in einem RFID-Rückgabeautomaten vorliegenden Leseanforderungen können mit einem Mid-Range-Leser abgebildet werden. Hier besteht die Möglichkeit entweder Leser mit einer integrierten Antenne oder mir einer abgesetzten Antenne zu verwenden. Um

eine sichere Lesung im gesamten Erfassungsbereich zu gewährleisten und Leselöcher zu schließen, empfiehlt es sich mehrere Antennen zu verbauen, welche der Reihe nach durchgeschaltet werden. Auf dem Markt sind verschiedene Leser verfügbar, welche die Möglichkeit zum Anschluss von mindestens zwei Antennen bieten. Da Rückgabeautomaten sich oftmals in einem geschlossenen Metallgehäuse befinden, sollte die Lesekammer nach allen Seiten hin mit einem Absorbermaterial ausgekleidet werden.

Zur Abbildung der Leseszenarien in Sortieranlagen können die gleichen Hardwarekomponenten verwendet werden, wie in den zuvor beschriebenen Rückgabeautomaten. Zu beachten ist allerdings, dass Sortieranlagen wesentlich großzügiger ausgelegt werden sollten, als es bei HF-Anwendungen der Fall ist. Grund dafür ist die wesentlich größere Lesereichweite eines UHF-Systems und mögliche Überreichweiten durch Reflektionen und die Weiterleitung von Wellen an Metall. Dies bedeutet, dass eine nahezu hundertprozentige Trennung von benachbarten Anlagen durchgeführt werden sollte. Beide Systeme sollten durch eine Schirmung voneinander getrennt werden. Ideal wäre es den Lesebereich mit Absorbermaterial in Form eines Tunnels auszukleiden. Es sollten sich keine Metallteile in der Nähe der Antenne befinden, in welches das Feld einkoppeln kann. Ebenso sollten die Rahmen der Förderanlagen, sowie alle Metallteile im gemeinsamen Bereich zweier Anlagen voneinander getrennt sein. Dadurch kann eine ungewollte Weiterleitung von Wellen vermieden werden. Zu beachten ist ebenfalls, dass nach Vereinzelung der Medien ein deutlich größerer Abstand zwischen diesen eingehalten werden muss, als es bei HF der Fall ist. Der Abstand zwischen zwei aufeinander folgenden Medien in der Förderanlage sollte 1m nicht unterschreiten. Nur so kann sichergestellt werden, dass eine eindeutige Erfassung und Zuordnung der Bücher und Medien erfolgen kann. Liegen die Artikel zu dicht aneinander, so kann es zu einer zeitgleichen Erfassung der Bücher kommen, wodurch eine automatische Sortierung unmöglich wird. Ebenfalls besteht die Möglichkeit, dass ein nachfolgendes Buch vor dem vorlaufenden erkannt wird. In diesem Fall käme es zu einer falschen Sortierung der Bücher. Um das Lesefeld weitestgehend auf den gewünschten Bereich zu beschränken, empfiehlt es sich, einen Tunnel aus absorbierenden Materialien um das Band herum zu errichten. Dies erfordert allerdings einen zusätzlichen Freiraum um die Anlage herum. Durch die Verwendung von speziellen Antennen mit geringem Öffnungswinkel kann das Antennefeld weiter konzentriert und beschränkt werden. Hier ist bereits eine Vielzahl so genannter 30°-Antennen auf dem Markt verfügbar.

Vermeidung von Stör- und Fehlerquellen bei der Installation eines HF-Systems

Grundsätzlich arbeiten heutige RFID-Geräte bei fachgerechter Installation zuverlässig und störsicher. Trotzdem sind dies Funkanlagen, welche durch andere Sender, starke Störer oder andere Störquellen beeinflusst werden können. Typische Fehlerquellen sind:

- Schlecht abgestimmte Antennen
- »Common Mode« Störungen bzw. Ströme
- Störungen von anderen Geräten (Monitore, Antriebe, Funkgeräte) in der Nähe
- Unzureichende Lesereichweite durch zu geringe Feldstärke

- Falsch abgestimmte oder zu kleine Transponder
- Ungewollte Lesungen
- Verringerung der Lesereichweiten durch gegenseitige Beeinflussung (Kopplung) der Transponder
- Gegenseitige Beeinflussung der RFID-Systeme durch andere in der unmittelbaren Umgebung
- Installationsfehler

Schlecht abgestimmte Antennen

Alle Antennen werden in der Regel vom Hersteller auf eine Impedanz von 50 Ohm abgestimmt. Sollten baulich bedingte Metallteile sich in der Nähe der Antenne befinden, kann ein zusätzlicher Nachgleich der Impedanz der Antenne notwendig werden. Die Impedanz kann mit Hilfe von Messgeräten überprüft werden. Ein nützliches Hilfsmittel zur Beurteilung der Anpassung der Antenne an die Impedanz von 50 Ω ist das VSWR Meter. Dieses Gerät misst das Verhältnis zwischen zugeführter und reflektierter Energie. Dabei gilt ein VSWR bis zu 1.3: 1 als guter Wert. Zur Messung wird die Antenne direkt über das Antennenkabel an ein SWR Meter angeschlossen.

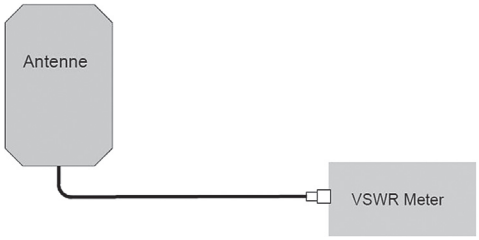


Abb. 13: Messung des SWR einer Antenne

Common Mode Störungen

Als Common Mode Störungen bezeichnet man Störungen von anderen elektrischen/elektronischen Geräten über das Erdpotenzial. Um diese zu vermeiden, sollten unbedingt die angegebenen Mindestabstände zum Metall beachtet werden. Metallteile in der Nähe der Antennen sollten gegebenenfalls sternförmig geerdet werden. Da es sich dabei um hochfrequente Störungen handeln kann, bietet es sich an dafür die Schirmung eines separaten Antennenkabels zu verwenden.

Abb. 14: Erdung über den Schirm eines zusätzlichen Antennenkabels

Bei der Installation sollten bereits im Voraus die Vorgaben des Herstellers und Hinweise in der Montageanleitung beachtet und in der Planung mit berücksichtigt werden. Durch die Montage von zusätzlichen Ferritringen an den Kabeln können Störungen ebenfalls um ein Vielfaches reduziert und unterdrückt werden. Um die Störanfälligkeit so gering wie nur eben möglich zu halten, sollten HF-Kabel und Energieleitungen in getrennten Rohren verlegt werden.

Störungen durch andere Geräte in der Nähe

Um Störungen durch andere Geräte in der Nähe der Installation zu vermeiden, sollten unbedingt alle angegebenen Mindestabstände beachtet werden. Dies gilt im Besonderen für Energieleitungen mit hoher elektrischer Leistung. Hier darf ein Mindestabstand von 1m nicht unterschritten werden. Ebenfalls können so auftretende Probleme durch die Verwendung einer zusätzlichen Schirmung und die Verlegung von Kabeln in getrennten Kabelrohren deutlich minimiert werden.

Unzureichende Lesereichweite durch zu geringe Feldstärke

Von entscheidender Bedeutung in diesem Fall sind die Eigenschaften des Lesers, der Antenne und des Transponders. Nur wenn diese optimal zueinander ausgewählt wurden, kann die bestmögliche Performance erzielt werden. Die angegeben maximalen Lesereichweiten des Herstellers sind zu beachten. In Abhängigkeit von der Größe und der Aktivierungsfeldstärke der ausgewählten Transponder müssen diese gegebenenfalls korrigiert werden. Um eine sichere Erfassung der Transponder in allen Fällen zu gewährleisten, sollten zur Sicherheit 10% von der angegebenen Lesereichweite abgezogen werden.

Falsch abgestimmte oder zu kleine Transponder

Transponder, Antenne und Leser bilden eine Einheit. Für mittlere und große Reichweiten müssen die Transponder eine minimale Größe haben. Die Empfindlichkeit der Transponder variiert in Abhängigkeit mit der Qualität. Es ist zu beachten, dass der Transponder durch das Einbringen in einem Buch oder auf einem Medium verstimmt wird. Unter Umständen kann dieser danach nicht mehr die gleiche Performance liefern, wie es zuvor der Fall war. Bei der Bestellung der Transponder sollte deshalb dem Labelhersteller der spätere Verwendungszweck mitgeteilt werden. Mittlerweile ist eine Vielzahl verschiedener Transponder auf dem Markt verfügbar, welche speziell für die Montage auf unterschiedlichen Materialien entwickelt wurden und erst die volle Performance in Kombination mit einem bestimmten Untergrund liefern. Tests mit mehreren der verwendeten Transpondern im Voraus sind sinnvoll.

Verringerung der Lesereichweite durch gegenseitige Beeinflussung (Kopplung) der Transponder

Um eine gegenseitige Beeinflussung der Transponder untereinander zu vermeiden, sollte zwischen diesen ein Mindestabstand eingehalten werden, der in etwa der Kantenlänge

bzw. dem Durchmesser des Transponders entspricht. Bei geringeren Abständen (z. B. dünne Büchern, CDs) ist mit einer wesentlich geringeren Empfindlichkeit zu rechnen. Hier müssen die Medien entweder vereinzelt oder RFID-Systeme mit höherer Leistung und Empfindlichkeit Verwendung finden.

Ungewollte Lesungen

Alle RFID-Antennen können Transponder in verschieden Ausrichtungen und Positionen zu der Antenne (z. B. über und unter der Antennenfläche) lesen. Treten ungewollte Lesungen auf, z. B. außerhalb eines Gates, so sollte die Anordnung der Antennen überprüft werden. Ebenso ist es möglich mittels einer zusätzlichen Schirmung den Lesebereich klar zu definieren. Unter Umständen kann mittels einer Reduktion der Sendeleistung der Lesebereich ebenfalls begrenzt werden. Hier sollte aber unter allen Umständen sichergestellt werden, dass die benötigte Lesereichweite in der Anwendung selbst sicher erzielt werden kann.

Gegenseitige Beeinflussung der RFID-Systeme durch andere in der unmittelbaren Umgebung.

Diese Probleme lassen sich oft durch die Einhaltung der angegebenen Mindestabstände, mit Hilfe von Multiplexern, Abschirmung der Antenne oder durch eine Synchronisation der Leser beheben.

Installationsfehler

Um installationsbedingte Fehler zu vermeiden ist es wichtig, dass alle Arbeiten in Übereinstimmung mit den nationalen Gesetzen und Bestimmungen für elektrische Anlagen sowie nach den örtlichen Vorschriften durchgeführt werden. Die Montageanleitungen der Antennen und Leser, sowie die Applikation-Notes des Herstellers sollten in jedem Fall mit berücksichtigt und darin enthaltene Hinweise umgesetzt werden. Dies gilt insbesondere für Angaben zu Mindestabständen, Kabellängen und zur Verlegung der Kabel.

Vermeidung von Stör- und Fehlerquellen bei der Installation eines UHF-Systems

Typische Fehlerquellen und Probleme, die bei der Installation eines UHF-Systems auftreten können, werden in dem folgenden Abschnitt gelistet und näher beschrieben.

- Interferenzen zwischen RFID-Systemen und anderen Funksystemen
- Beeinflussung des RFID-Systems durch andere elektronische Geräte und Felder
- Beeinflussung der RFID-Systeme untereinander bei zu starker Kopplung
- Reflektionen und Absorptionen
- Überreichweiten durch die Weiterleitung von Wellen
- Zu kleine oder schlecht abgeglichene Transponder

Interferenzen zwischen RFID-Systemen und anderen Funksystemen

Der Standard EN 302208 reserviert in Europa ein Frequenzband von 865 -868 MHz exklusiv für RFID-Anwendungen im UHF-Bereich. Da es sich bei diesem Bereich nur um einen Ausschnitt des ISM-Bandes handelt, sind auf benachbarten Frequenzen eine Vielzahl anderer Funksysteme angesiedelt. Dadurch kann es zu einer gegenseitigen Beeinflussung der verschiedenen Anwendungen und Systeme kommen. Systeme, welche auf ähnlichen Frequenzen arbeiten, können verschiedene Messsysteme, wie sie beispielsweise zum Auslesen von Stromzählern eingesetzt werden, oder Funkthermometer sein. Ebenso betroffen sind davon sicherheitsrelevante Geräte, wie beispielsweise Brandmeldeanlangen. Befindet sich eine UHF-Antenne in der Nähe eines solchen Gerätes, so kann es zu einem Ausfall dessen, beziehungsweise zu einer Störung der Funkverbindung dieser Geräte kommen. Besonders kritisch ist dies bei sicherheitsrelevanten Systemen, wie Brandmeldeanlagen oder Alarmanlagen. Umgekehrt senden diese Geräte teilweise ein recht breitbandiges Signal, welches wiederum die Leser-Transponder-Kommunikation empfindlich stören kann. Besonders kritisch ist dies, wenn ein solches Signal die Transponderantwort überlagert. In diesem Fall ist eine Identifikation des Transponders unmöglich. Um dies auszuschließen, sollte das Spektrum im Frequenzbereich von 860 MHz bis 870 MHz mit Hilfe eines Spektrum-Analyzers überprüft werden. Wichtig ist hierbei die Messung zu einem Zeitpunkt durchzuführen, wenn alle möglichen Störsysteme eingeschaltet sind.

Beeinflussung des UHF-Systems durch andere elektronische Geräte und Felder

Leuchtstoffröhren, Computermonitore und andere elektronische Geräte strahlen oftmals starke Felder ab. Diese können die Funktion eines UHF-RFID-Systems erheblich beeinträchtigen. Kritisch ist dies jedoch nur, wenn die Antenne in unmittelbarer Nähe eines solchen Gerätes installiert wird. Wird beispielsweise eine Antenne neben einer Leuchtstoffröhre installiert, so kann es sein, dass, während die Leuchte eingeschaltet ist, die Lesereichweite drastisch zusammenbricht. Im Gegenzug kann aber auch eine Beeinflussung anderer Geräte durch ein RFID-System nicht ausgeschlossen werden. Dies ist beispielsweise bei Computermonitoren der Fall. Wird eine Antenne in unmittelbarer Nähe eines Monitors in Betrieb genommen, so kann es zu Verzerrungen und Flimmern des Bildschirms kommen. Grundsätzlich gilt, dass zwischen RFID-Systemen und anderen elektronischen Geräten ein Mindestabstand von 80cm eingehalten werden sollte, damit gegenseitige Wechselwirkungen ausgeschlossen werden.

Beeinflussung der UHF-Systeme untereinander

Hauptursache für eine gegenseitige Beeinflussung von UHF-RFID-Systemen untereinander ist eine Übersteuerung des Empfängers eines Lesers. Dies ist der Fall, wenn ein zu starkes Signal in den Empfangszweig eines Lesers gekoppelt wird. Wie stark dieses Signal sein darf, kann nicht genau spezifiziert werden und ist abhängig von den Eigenschaften des Lesers. Genauere Auskunft kann der Hersteller des verwendeten Gerätes geben. Grundsätzlich kommt es zu einer Übersteuerung, wenn zwei Antennen von zwei

unabhängigen Lesern direkt parallel zueinander ausgerichtet sind. Dies ist typischerweise der Fall bei zwei eng zusammenstehenden Gates. Bei solchen Installationen sollte ein Mindestabstand von zwei parallel zueinander ausgerichteten Antennen von mindestens 8m nicht unterschritten werden. Um in solchen Situationen einer Übersteuerung entgegen zu wirken, sollte die Ausgangsleistung des Lesers soweit wie eben möglich reduziert werden. Ebenso kann in diesem Fall versucht werden die Returnlink Bitrate soweit wie möglich zu reduzieren. Dies bringt den Vorteil, dass die Eingangsfilter des Empfängers schmalbandiger werden und Störungen in einem etwas geringerem Maße eingekoppelt werden. Ebenfalls sollten die Leser getriggert werden. Dies kann beispielsweise durch einen Bewegungsmelder oder eine Lichtschranke erfolgen. Dadurch ist ein Leser nur dann aktiv, wenn dies unbedingt erforderlich ist. Dies hilft allerdings nicht eine gegenseitige Beeinflussung zu vermeiden. Eine Triggerung trägt lediglich dazu bei die Wahrscheinlichkeit für eine gegenseitige Beeinflussung zu reduzieren, da beide Leser gleichzeitig aktiv sein müssen.

Optimalen Erfolg versprechen jedoch eine zusätzliche Schirmung, bzw. eine Wand aus Absorbermaterialien zwischen beiden Antennen. Hierdurch wird eine Kopplung zwischen beiden Systemen nahezu vollständig unterbunden.

Sind zwei Antennen eines Lesers in paralleler Ausrichtung zueinander montiert, so bleibt dies ohne Auswirkungen. Verantwortlich hierfür ist ein im Leser integrierter Multiplexer, durch welchen die Antennen der Reihe nach geschaltet werden.

Reflektionen und Absorptionen

Reflektionen und Absorptionen sind am häufigsten auftretende Störgrößen in UHF-Applikationen. Oftmals treten Reflektionen und Absorptionen gleichzeitig auf. Wie zuvor bereits beschrieben, werden Reflektionen durch alle Gegenstände und Oberflächen in einem Gate und um ein Gate herum verursacht. Durch Reflektionen kommt es zu einer Überlagerung von Wellen, wodurch Leselöcher entstehen können. Um eine sichere dreidimensionale Erfassung in einem Gate zu ermöglichen, sollte deshalb unter allen Umständen mit mehreren Antennen gearbeitet werde. Ebenso sollte es vermieden werden Gegenstände dauerhaft im Bereich eines Gates abzustellen. Dies gilt insbesondere für metallische Gegenstände die Reflektionen begünstigen. Ebenso kritisch wie Metallteile sind Flüssigkeiten, die sich im Bereich vor den Antennen befinden. Wasser und andere Flüssigkeiten sowie Klebstoffe oder verschiedene Gummisorten besitzen die Eigenschaft Funkwellen zu absorbieren und eine Identifikation der dahinter liegenden Transponder zu verhindern.

Überreichweiten durch die Weiterleitung von Wellen

Funkwellen im UHF-Frequenzband können an der Oberfläche von großen Metallteilen aufgenommen und weitergeleitet werden. Dadurch können gegebenenfalls extreme Überreichweiten von bis zu 50m erzielt werden. Typischerweise tritt die Weiterleitung von Wellen an baulich bedingten Metallteilen auf. Die können zum Beispiel Stahlträger,

Stahlbeton oder Heizungsrohre sein. Ebenso davon betroffen sind nachträglich installierte Metallteile, wie beispielsweise Förderanlagen oder große Maschinen. Zur Vermeidung eines solchen Phänomens sollten alle Metallteile in der Nähe einer Antenne abgeschirmt werden.

Zu kleine oder schlecht abgeglichene Transponder

Wie im HF-Bereich können dicht beieinander liegende Transponder eine Wechselwirkung aufeinander haben. Je dichter diese zusammen liegen, desto größer ist die gegenseitige Verstimmung. Auch kann eine Identifikation von Transpondern durch darüberliegende Transponder vermieden werden. Die Antennenfläche eines Transponders besteht aus Metall. Liegen mehrere Transponder dicht gedrängt übereinander, so kann es zu einer Abschirmung der unteren Transponder kommen.

Eine Verstimmung der Transponder erfolgt auch durch das Material, auf welchem sie aufgebracht werden. Liegt die Resonanzfrequenz eines Transponders unter idealen Bedingungen gewöhnlich bei 865 MHz, so kann diese durch die Aufbringung auf verschiedenen Materialien stark verschoben werden. Durchgeführte Tests haben ergeben, dass beispielsweise die Resonanzfrequenz eines Transponders nach Aufbringung in einem Buch um bis zu 200 MHz herabgesenkt werden kann. Eine solche Verschiebung der Resonanzfrequenz hat auf die grundsätzliche Funktion eines Transponders keinen Einfluss. Hierdurch wird jedoch die maximal mögliche Performance des Transponders bei der gesetzlich vorgeschriebenen Betriebsfrequenz verringert. Um solche Phänomene zu verhindern, sind verschiedene, speziell vorverstimmte Transponder auf dem Markt verfügbar. Diese werden durch das Material, auf welchem sie aufgebracht werden, richtig gestimmt und zeigen in Kombination mit dem speziellen Untergrund erst die bestmögliche Performance.

Fazit

Stellt man die Eigenschaften der HF-Technologie und der UHF-Technologie gegenüber, so ist zuerkennen, dass beide RFID-Systeme Ihre Vor- und Nachteile besitzen.

Der große Vorteil der UHF-Technologie besteht dabei in der hohen Reichweite, welche erzielt werden kann. Problematisch ist allerdings, dass es bedingt durch Reflektionen zu Leselöchern und Überreichweiten kommen kann. Das Feld lässt sich nur sehr schwierig und aufwändig begrenzen. Um eine dreidimensionale Erfassung zu ermöglichen, muss mit mehreren Antennen gearbeitet werden.

Mit einem HF-System ist die maximale Lesereichweite deutlich geringer. Dafür besitzt ein HF-System den Vorteil, dass durch das Prinzip der induktiven Kopplung ein sehr homogenes Feld aufgebaut wird, in dem der Transponder sicher erkannt werden kann. HF-Antennen werden vom Hersteller auf eine Impedanz von 50 Ohm angepasst. Dieser Impedanzwert sollte aber nach erfolgter Installation der Antennen nochmals überprüft werden. Gegebenenfalls muss die Antenne nachgeglichen werden. Bei einem

UHF-System erfolgt eine derartige Beeinflussung der Antenne nicht. Somit kann auf eine zusätzliche Überprüfung der Antennen verzichtet werden.

Kritisch für den Betrieb beider Systeme sind Metalle in der Nähe der Installation. Bei HF wirken sich Metalle sehr stark auf die Impedanz der Antenne aus und verstimmen diese. Nach Einhaltung der zuvor angegeben Mindestabstände und einem durchgeführten Antennenabgleich ist dieser Einfluss jedoch nahezu kompensiert und das System stabil. Im UHF-Bereich werden durch Metalle zusätzliche Reflektionen verursacht, wodurch eine sichere Erfassung des Transponders im gesamten Durchgangsbereich problematisch werden kann. Auch werden bei einem UHF-System durch kleinste Änderungen im Erfassungsbereich die Eigenschaften des Feldes stark beeinflusst. Dies können beispielsweise Personen sein, welche durch das Gate hindurchgehen oder Pflanzen, welche zur Dekoration aufgestellt werden. Mit jeder Änderung der Umgebungsbedingungen entstehen neue Reflektionen, wodurch es zu einer Verschiebung des Antennenfeldes kommen kann. Es entstehen neue Leselöcher. Dadurch lässt sich die Ausbreitung eines UHF-Feldes niemals genau vorhersagen und berechnen.

Auf Grund der Vielzahl von Erfahrungen, welche bereits mit HF-Systemen im Bibliotheksumfeld gesammelt wurden und der hohen Anzahl von erfolgreich installierten Systemen wäre die HF-RFID-Technologie nach dem jetzigen Stand der Technik für RFID-Installationen in Bibliotheken zu bevorzugen.

Automation zwischen Insellösung und Logistikkreislauf

RFID-gestützte Verknüpfung verschiedener Komponenten als erste Stufe automatisierter Logistikkonzepte in Bibliotheken

Olaf Eigenbrodt

Der Beitrag erläutert anhand der Koppelung von Medienrückgabe, Sortierung und Transport im Jacob- und Wilhelm-Grimm-Zentrum, dass die Verknüpfung verschiedener automatisierter Komponenten ein erster Schritt in Richtung auf Logistikreisläufe in Bibliotheken sein kann. Voraussetzungen und Entwicklung RFID-gestützter automatisierter Kreisläufe werden im zweiten Teil an Beispielen skizziert.

Einleitung

Für den Einsatz von RFID wurden und werden im Bibliotheksbereich immer neue Anwendungen definiert. Die Verbindung zweier klassischer Probleme der Automatisierung von Routineaufgaben in Bibliotheken – die Identifizierung von Medien zur elektronischen Verbuchung ohne manuelle Eingabe von Identifikationsnummern o. ä. und die Sicherung der Medien gegen unerlaubtes Entfernen aus den Bibliotheksräumen – ist sicherlich für viele Anwender die wesentliche Motivation zur Umstellung auf RFID. Die Technik ermöglichte damit erstmals eine relativ einfache, nutzerfreundliche und zügige Selbstverbuchung von Medien bei geringer Fehleranfälligkeit.

Ähnlich wie die nur unwesentlich ältere aber im Bibliothekswesen schon länger in Einsatz befindlichen Barcodes hat aber die RFID-Technik ein Potential, das wesentlich weiter reicht. Schon früh wurden zusätzliche Anwendungen, wie die automatisierte Inventur bzw. Revision der Bestände oder das Auffinden verstellter Bücher im Bestand beworben. Dabei übernehmen die Bibliotheken in der Regel Anwendungen des Einzelhandels zur Sicherung von Waren sowie zur eindeutigen Identifizierung des individuellen Stücks oder der Warengruppe bei der Transaktion an den Kunden oder der Inventur. Barcode und RFID werden aber schon immer intensiv auch im Bereich der Logistik eingesetzt, wo sie für die effiziente und automatisierte Lagerung genauso eingesetzt werden wie für einen zielgenauen und zeitsparenden Transport. Der reibungslose und genau getaktete Betrieb der Logistik in Handel und produzierendem Gewerbe wäre heute ohne diese Technik nicht mehr vorstellbar. Die eingesetzten Systeme reichen dann von passiven RFID-Transpondern, wie wir sie aus Bibliotheken kennen bis zu aktiven Real-Time-Locating-Systemen (RTLS), wie sie etwa im Containerumschlag verwendet werden. Parallel wird auch immer noch mit Barcodes gearbeitet, wobei die geringere Informationsdichte für die individuelle Verfolgung eines Produkts von der Vorproduktion bis zum Endverbraucher ungeeignet ist, da hier in der Regel nur Chargen verfolgt werden können.

Auch Bibliotheken müssen diverse Logistikaufgaben lösen, um einwandfrei arbeiten zu können. Im Zuge der wichtigen und nachvollziehbaren Wandlung von einer verwaltungszentrierten zu einer nutzerorientierten Organisation, die unter anderem auch durch den Einsatz von RFID-Technik im Nutzungsbereich unterstützt wird, wird der Aspekt einer reibungslosen Logistik manchmal vergessen. Die führt dazu, dass gerade größere Bibliotheken mit umfangreichen Magazinbeständen im Bereich der Aushebung, des Transports und der Bereitstellung von Materialien, aber natürlich auch bei der Rücknahme, beim Rücktransport ins Magazins und beim Zurückstellen der Materialien, oft noch mit Techniken und Prozessen des 20. oder gar 19. Jahrhunderts arbeiten, obwohl sie im Nutzungsbereich selber längst Technik des 21. Jahrhunderts anbieten.

In diesem Beitrag geht es darum, wie man unterstützt durch den Einsatz von RFID von technisch oft nicht mehr zeitgemäßen Insellösungen zu effizienten Logistikketten kommt, die sich in Bibliotheken meist als Kreisläufe darstellen. Einen Zwischenschritt auf diesem Weg stellen Anlagen wie die im Jacob-und-Wilhelm-Grimm-Zentrum eingesetzte Kombination von Medienrücknahme, -Sortierung und -Transport dar. Deshalb werde ich im Folgenden Vorgeschichte, Konzept und Funktion dieser Anlage im Gesamtkonzept des Hauses vorstellen, bevor ich ein RFID-gestütztes Konzept einer Logistikkette umreiße. In einem Ausblick möchte ich dann noch auf denkbare Logistiklösungen auch für kleinere Bibliotheken eingehen.

Verknüpfung von Komponenten im Jacob-und-Wilhelm-Grimm-Zentrum

Als eine der ersten Bibliotheken in Deutschland erhielt die Universitätsbibliothek der Humboldt-Universität zu Berlin für ihre neue Zentralbibliothek, das Jacob-und-Wilhelm-Grimm-Zentrum, eine kombinierte Anlage für Medienrücknahme, -Sortierung und -Transport. Die Verknüpfung dieser drei Komponenten scheint zunächst naheliegend, war aber mit einigen Diskussionen und Herausforderungen verbunden und hatte auch eine Vorgeschichte, auf die ich im Folgenden kurz eingehen möchte.

Von Hasen, Igeln und Selbstverbuchung

Die Eröffnung des Erwin-Schrödinger-Zentrums auf dem Mathematisch-Naturwissenschaftlichen Campus der Humboldt-Universität zu Berlin in Berlin-Adlershof im Jahre 2003 war ein wesentlicher Entwicklungsschritt der Universitätsbibliothek hin zu einer verstärkten Automatisierung bibliothekarischer Prozesse – allerdings mit unterschiedlichem Erfolg. Damals verzichtete man auf die Einführung von RFID-Technik sowohl im Nutzungsbereich als auch in der Logistik. Im Jahr darauf führte die Universitätsbibliothek der Technischen Universität Berlin RFID zunächst in ihrer Lehrbuchsammlung ein. Im Bereich der Logistik entschied man sich im Erwin-Schrödinger-Zentrum aus Gründen der Gebäudegeometrie- und wegen der damit verbundenen Kostenprognose für eine Kastenförderanlage für ein Fahrerloses Transportsystem (FTS), das unter dem Namen »Hase und Igel« zumindest im deutschen Bibliothekswesen einige Berühmtheit erlangte. Trotz dieser Bekanntheit blieb »Hase und Igel« eine Sonderentwicklung, die als ein Kuriosum des auf ein hochmodernes technisches Erscheinungsbild bedachten Hauses und nicht

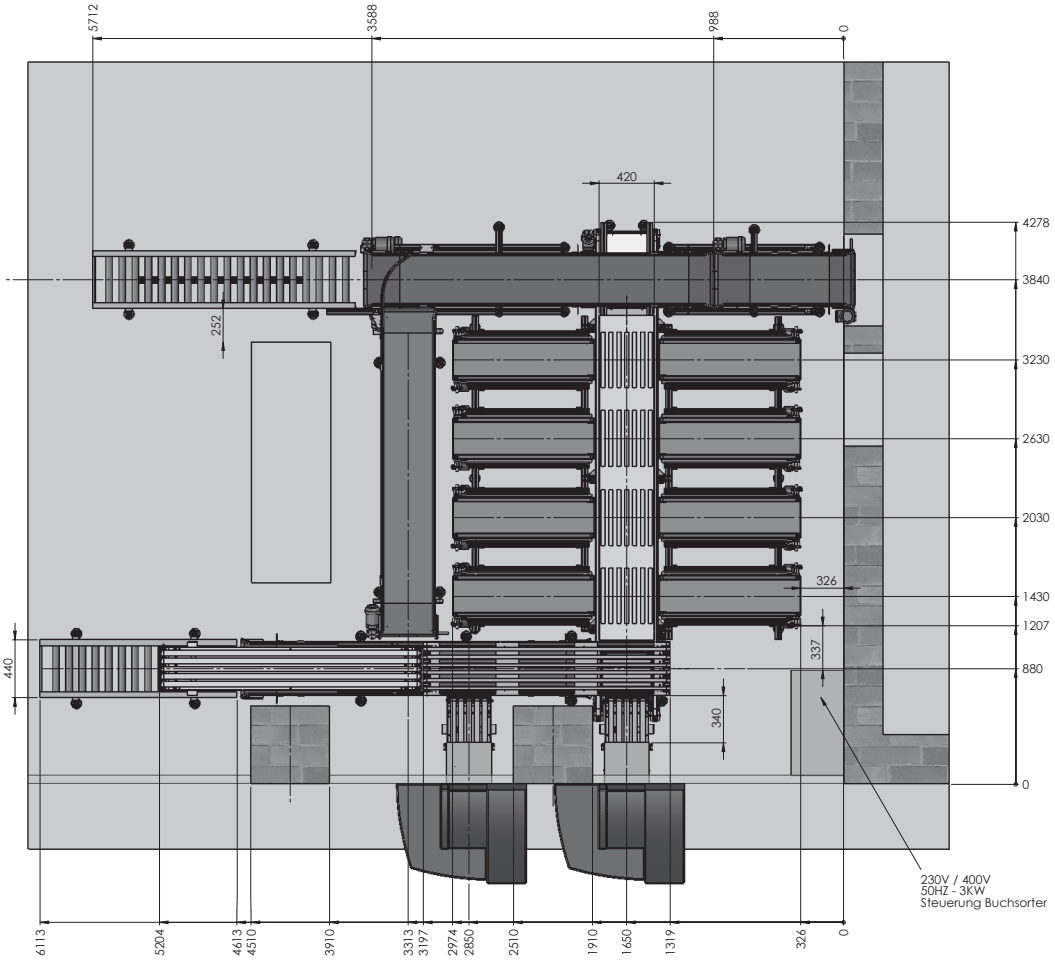


Abb. 1: Aufbau der gekoppelten Anlage im Jacob-und-Wilhelm-Grimm-Zentrum (Zentralbibliothek der Humboldt-Universität zu Berlin)

als eine für die Logistik in Bibliotheken denkbare Entwicklung gesehen wurde. Andreas Richter sieht den Einsatz solcher Systeme in einem eher deskriptiven Beitrag zu Förder- und Sortiertechniken folgerichtig auch als problematisch an [vgl. 1, S. 179 f.]. Auf die Möglichkeiten, die ein solches System in der Logistikkette gerade größerer Magazinbibliotheken bieten könnte, geht er leider nicht ein.

Sowohl »Hase und Igel« als auch die im Erwin-Schrödinger-Zentrum eingesetzten Selbstverbuchungsgeräte blieben allerdings Insellösungen. Die Selbstverbuchungsgeräte wurden nach diversen Problemen mit Technik und Bedienerfreundlichkeit der Geräte gar nicht mehr genutzt, während das FTS nach der Beseitigung einiger ‚Kinderkrankheiten' heute seinen geregelten Dienst verrichtet. Durch die erfolgreiche Einführung von RFID im Rahmen des Projekts PROFILE HU verfügt das Erwin-Schrödinger-Zentrum inzwischen über einen Rückgabeautomaten mit angeschlossener Sortieranlage allerdings ohne Koppelung an das FTS.

Konzept der gekoppelten Anlage im Jacob-und-Wilhelm-Grimm-Zentrum

Schon bei der Fertigstellung des Erwin-Schrödinger-Zentrums stand fest, dass dies nicht der letzte Neubau der Humboldt-Universität für Bibliothek und Computer- und Medienservice bleiben würde. 2004 wurde der Architekturwettbewerb für das Jacob-und-Wilhelm-Grimm-Zentrum durchgeführt. Schon in der Ausschreibung für den offenen Realisierungswettbewerb, die die Humboldt-Universität in Zusammenarbeit mit der Senatsverwaltung für Stadtentwicklung erstellte, hatte die Buchtransportanlage sowohl in den Flächenanforderungen als auch in der Beschreibung der Technischen Gebäudeausrüstung eine herausgehobene Stellung [2, S. 58 bzw. 70], auch die Notwendigkeit von Selbstverbuchungsanlagen wurde an dieser Stelle schon erwähnt. Der Einsatz von RFID hingegen wurde zu diesem Zeitpunkt intern zwar diskutiert, war aber noch nicht entschieden. Kostenargumente im Hinblick auf die Gesamtgröße des Bestandes spielten in diesen Diskussionen genauso eine Rolle, wie die damals in den Augen vieler Beteiligter noch nicht ausgereifte Technik.

Im Rahmen der Vorplanung kam man dann relativ schnell zu dem Schluss, dass man die Buchrückgabe nicht nur durch eine Sortieranlage weiter automatisieren, sondern auch an die Transportanlage koppeln sollte. Aufgrund des als geographischer Standort idealen aber für die Gebäudegeometrie schwierigen Baugrundstücks mussten alle Entwürfe zwangsläufig in die Höhe gehen. Der Siegerentwurf des Schweizer Architekten Max Dudler setzte sich über die in der Ausschreibung empfohlene Beachtung der umliegenden Traufhöhen hinweg und erreicht im südlichen Gebäudeteil eine Höhe von 9 Geschossen plus Untergeschoss. Damit war die maximal denkbare Höhenentwicklung allerdings erreicht und man musste mit relativ niedrigen Deckenhöhen arbeiten, um die vorhandenen Höhen optimal auszunutzen. Zum Beispiel wurden alle Leitungen in den Fußboden verlegt, so konnte auf eine Abhangdecke verzichtet werden. Diese konstruktiven Vorgaben und architektonischen Entscheidungen machten eine horizontale Buchtransportanlage konstruktiv und damit auch finanziell zu aufwändig, so dass auf diese verzichtet werden musste. Wegen der geringen Gebäudetiefe wurde dies auch weniger kritisch gesehen, als die Verteilung auf die Gebäudelänge. Stattdessen entschied man sich deshalb für eine vertikale Buchtransportanlage mit zwei Aufzügen.

In diesem Zusammenhang kam dann die Koppelung der mit dem Rücknahmeautomaten verbundenen Sortieranlage mit der Transportanlage ins Gespräch. Während auf der einen Seite ein erheblicher Personalaufwand durch die Verteilung und das Rückstellen der Medien in einem großen Freihandbereich mit einer Kapazität von bis zu 2 Millionen Bänden sicher zu erwarten war und als Organisationsproblem des Freihandbereichs sehr früh thematisiert wurde, wollte man andererseits im Bereich der Sortierung und auch körperlich anstrengenden Umsetzung auf die Kastenförderanlage Personal sparen. Die Idee der Koppelung von Rücknahme, Sortierung und Transport lag damals im Trend und wird auch bei anderen Projekten, die in dieser Zeit geplant und jetzt realisiert wurden eingesetzt.

Konzeptionell stand schnell fest, dass die gesamte Rückgabe der Medien vom Auflegen des Mediums auf das Förderband des Automaten durch den Nutzer bis zur Ankunft des Transportkastens auf der richtigen Etage inklusive einer Benachrichtigung des Personals

automatisiert werden sollte. Neben der damals also schon gängigen Reduzierung des Sortieraufwands und der erwähnten Umsetzung auf die Förderanlage wurden auch die Zieleingabe der Kästen und die Bestückung der Sortieranlage mit Leerkästen automatisiert. Hier stellten sich für den Bibliotheksbereich völlig neue funktionale Anforderungen.

Funktion der Anlage

Die drei grundlegenden Komponenten der Anlage – Rücknahmeautomat, Sortieranlage und Kastenförderanlage – sind für sich genommen nicht neu im Bibliotheksbereich, wobei alle drei Lösungen zunächst als Insellösung existierten.

Rücknahmeautomaten können sowohl mit Barcodes als auch mir RFID arbeiten und verbuchen zurückgegebene Medien nach Identifizierung im System der Bibliothek. Hier ist die Schnittstelle zwischen dem Gerät und dem Ausleihmodul der Bibliothekssoftware ein entscheidender Faktor. Rücknahmeautomaten wurden und werden primär dort eingesetzt, wo bis dahin mit Klappenrückgaben für Medien gearbeitet wurde. Der Automat hat für Nutzerinnen und Nutzer den Vorteil, dass zurückgegebene Medien im System verbucht werden. Bibliotheken profitieren ebenfalls von der sofortigen Verbuchung und der relativ höheren Sicherheit vor Vandalismus gerade bei Geräten für einen 24/7-Service, die im Außenbereich angebracht werden. Eine automatisierte Rückgabe über Selbstverbuchungsgeräte war und ist in vielen Bibliotheken schon länger möglich. Hier müssen Kundinnen und Kunden die Medien allerdings selbst auf Bücherwagen ablegen, diese ‚verschwinden' nicht in einem Hintergrundarbeitsbereich. In immer mehr Bibliotheken entschließt man sich daher, Rücknahmeautomaten auch im Innenbereich der Bibliothek einzusetzen.

Die Idee, einen Rücknahmeautomaten mit einem Sortierer zu verbinden, liegt eigentlich nahe, wenn es sich um große Bibliotheken oder Bibliothekssysteme mit mehreren Standorten handelt. Allerdings sind auch andere Lösungen denkbar. So werden etwa im Bibliothekssystem Singapurs über Automaten zurückgegebene Medien manuell vorsortiert und dann zur Sortieranlage der Post geliefert, von wo die sortierten Medien dann wieder auf die Standorte verteilt werden. Neben dem entstehenden Transportaufwand hat dieses System auch den Nachteil, dass die Medien manuell vorsortiert und am Zielort noch einmal feinsortiert werden müssen. Allerdings gibt es auch international diverse Beispiele für die gelungene Verbindung von gekoppelter Medienrückgabe und –sortierung. In der Planungsphase der Anlage im Grimm-Zentrum wurden sowohl Anwendungen in Deutschland (Stadtbibliothek München) als auch in Dänemark angesehen. Die Schnittstelle braucht hier zusätzlich Informationen, die bei einem reinen Rückgabeautomaten nicht abgerufen werden müssen: Standort des Exemplars zur richtigen Zuordnung, ggf. Vormerkungen etc. Zudem entschied man sich, zwei Rückgabeautomaten mit der Sortieranlage zu verbinden, was die Komplexität der Sortierung noch erhöht. Die Standardanlagen in diesem Bereich arbeiten in der Regel entweder mit großen Wagen, die über einen Federboden verfügen und so materialschonend relativ hohe Kapazitäten aufweisen (Gerade für den Nacht- oder Sonntagsbetrieb wichtig) oder sie übergeben die Medien direkt an spezielle Bücherwagen, die zwar weniger Kapazität haben, aber direkt weggefahren und in die richtige Abteilung der Bibliothek gebracht werden können.

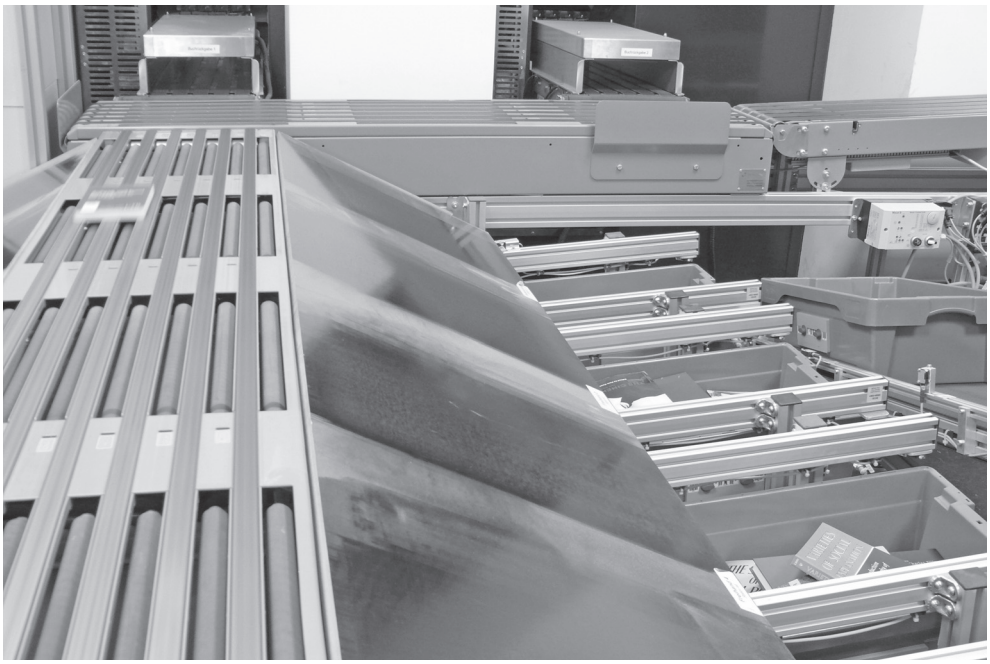


Abb. 2: Die Koppelung von Buchrücknahme, -sortierung und -transport als erster Ansatz eines Logistikkreislaufs

Beide Lösungen haben jedoch Nachteile. So müssen die sortierten Medien entweder in der Nähe der Sortieranlage oder vor Ort noch einmal manuell umgepackt werden. Im Münchener Beispiel geschieht dies sogar zweimal – einmal werden die Medien in die Kästen der Kastenförderanlage sortiert, dann am Zielort noch einmal zum Rückstellen.

Zumindest den ersten Vorgang wollte man sich im Jacob-und-Wilhelm-Grimm-Zentrum durch eine direkte Koppelung an die Kastenförderanlage ersparen. Die Medien werden nicht mehr in spezielle (Bücher-)wagen sortiert, sondern direkt in die Kästen der Förderanlage. Hier entstehen zusätzliche Anforderungen an das System. Zunächst muss eine Schnittstelle zwischen der Sortieranlage und dem Transportsystem geschaffen werden. Zum Zeitpunkt der Planung der Anlage für das Jacob-und-Wilhelm-Grimm-Zentrum gab es keinen Anbieter, der diese Lösung aus einer Hand hätte realisieren können. Alle Bieter im Verfahren arbeiteten mit einem weiteren Partner zusammen. Die Koppelung von Rücknahme und Sortierung war wie erwähnt schon gängig, diese schon vorhandenen Systeme mussten also mit einer Transportanlage verbunden werden. Neben dem Datenaustausch waren auch mechanische Fragen zu lösen: Wie kann man mit Standardtransportkästen arbeiten, ohne die Belastung für die Materialien zu groß werden zu lassen? Was geschieht während der Phase, in der ein voller Kasten abgeholt und gegen einen leeren ausgetauscht wird? Kann die Geschwindigkeit der Transportanlage mit der Kapazität der an zwei Rückgabeautomaten angeschlossenen Sortieranlage mithalten? Gerade die Frage der Bestandserhaltung spielt in einer Wissenschaftlichen Bibliothek mit einer gewissen Archivfunktion quantitativ eine größere Rolle als in einer Öffentlichen Bibliothek, die ihre Materialien in der Regel irgendwann sowieso austauscht.

Abb. 3: Zusätzliche manuelle Zuführung von Medien an der Anlage im Jacob-und-Wilhelm-Grimm-Zentrum

Der Planungsprozess erforderte demnach von allen Beteiligten einen hohen Zeit- und Personalaufwand. Neben der Erstellung von Pflichtenheften, der Sammlung zusätzlicher Anforderungen und Detailkonfigurationen mussten auch die Anforderungen an die Schnittstelle zum Aleph-System genau definiert werden. Hinzu kamen Simulationen, Werksbemusterungen von Komponenten und die erwähnten Besuche bereits im Betrieb befindlicher Anlagen.

Entstanden ist eine Anlage mit zwei Rückgabeterminals und acht Sortierungen, die die vollen Kästen über einen Aufzug auf sieben Etagen verteilt und über einen achten Kasten verfügt, der nicht eindeutig zuzuordnende Materialien genauso übernimmt, wie diejenigen Medien, die während des Austausches eines Kastens nicht in diesen zugeordnet werden können. Neben den beiden Rückgabeautomaten verfügt die Anlage noch über eine manuelle Zuführung, die es den Mitarbeiterinnen und Mitarbeitern der Leihstelle ermöglicht, unsortierte Medien von der Sortier- und Transportanlage verteilen zu lassen. Der Füllstand der einzelnen Kästen in der Anlage wird automatisch detektiert und der Kasten bei Bedarf abtransportiert. Die Anlage verfügt über eine eigene Aufzugsstation, der Kasten wird dort übernommen und auf die Etage transportiert, zu der er zugeordnet ist. Hier stehen in der Regel lange Stationen zur Verfügung, die mehrere Kästen aufnehmen können. Sowohl über die VoIP-Telefonanlage als auch über ein Interface auf dem Arbeitsplatzrechner ist der Füllstand der einzelnen Stationen kontrollierbar. Nach der Leerung durch das Bibliothekspersonal werden die Kästen wieder in das System zurückgegeben. Sollte eine Station abends oder am Wochenende volllaufen, können die Kästen in einem Pufferspeicher im Keller zwischengelagert werden, ist die entsprechende

Station wieder leer, werden die Kästen von dort abgerufen. Ein Leerbehälterspeicher sorgt für eine reibungslose Versorgung mit leeren Kästen. Die Sortieranlage selbst hält immer leere Behälter bereit, um abtransportierte zu ersetzen, wird dort ein Behälter abgerufen, holt sich die Anlage aus dem Leerbehälterspeicher einen neuen.

Herausforderungen und Schwierigkeiten

Obwohl wie beschrieben von vorn herein der Wunsch nach einer Transportanlage und nach automatisierter Medienverbuchung bestand, wurden Typ und Art der Anlage bewusst offen gelassen, um die Marktentwicklung und den technischen Fortschritt in diesem Bereich abzuwarten. Die Entscheidung zur Koppelung beider Systeme über die Sortieranlage wurde dann zwar zu einem relativ frühen Zeitpunkt getroffen, einige wesentliche Entscheidungen zur Gebäudegeometrie, vor allem auch zu den Verkehrsflächen im Erdgeschoss, waren da aber schon gefallen. In Verbindung mit Verzögerungen bei der Vergabe führte dies dazu, dass zum Zeitpunkt der Auftragserteilung nur noch eine relativ kleine und vor allem auch fest begrenzte Fläche zur Verfügung stand. War die sich dadurch ergebende Kompaktheit der Anlage zunächst eine Herausforderung für die ausführenden Firmen und erst in zweiter Linie ein Problem für die spätere Wartung und Bedienung, so waren die damit verbundene Begrenzung der Sortierungen auf acht und die fehlende Erweiterbarkeit der Anlage ein unmittelbares Planungsproblem. Wie sich schnell herausstellte, wären zur optimalen Vorsortierung der Medien mindestens zwölf Sortierplätze notwendig gewesen. Zusätzlich zu den zu versorgenden Etagen mit ausleihbarem Bestand (UG, EG, 2.-5. OG, 7. OG) hätte man für eine optimale Entlastung des Personals noch Sortierungen für vorgemerkte Medien, Medien anderer Standorte (evtl. mit einer internen Sortierung für einzelne große Standorte oder Fahrtrouten) und nicht eindeutig zuzuordnende Medien gebraucht. Letztere waren zumindest in der Anfangsphase in Folge der Zusammenführung der Bestände aus 13 bis dahin im System selbständig geführten Standorten noch relativ häufig. Hier wäre ein Ansatz zur Weiterführung der automatisierten Logistikkette gewesen, auf den ich später noch eingehen möchte.

Eine besondere Herausforderung stellte die sich relativ spät ergebende Gelegenheit der RFID-Einführung an der Universitätsbibliothek der Humboldt-Universität zu Berlin dar. Trotz der unbefriedigenden Perspektive, die Automatisierung auf der Grundlage der vorhandenen Barcode-Technik voranzubringen, war man aus Kostengründen gezwungen, die im Jacob-und-Wilhelm-Grimm-Zentrum zunächst geplante Einführung von RFID zu verschieben. Durch das vom Europäischen Fond für Regionale Entwicklung (EFRE) geförderte Projekt PROFILE-HU ergab sich die Gelegenheit, die geplante Serviceverbesserung durch Automatisierung auch konsequent umzusetzen und RFID im gesamten Bibliothekssystem der HU einzuführen. So erfreulich diese Entwicklung war, so sehr bedeutete sie auch einen Kraftakt für alle Beteiligten [vgl. dazu und zum Projektverlauf 3]. Insbesondere die Einpassung der bereits geplanten Medienrücknahme, -Sortierungs und -Transportanlage in zwei Projektumgebungen bedeutete einen organisatorischen und technischen Mehraufwand. Hinzu kam, dass man sich im Gegensatz zu den anderen – bedeutend kleineren – Standorten der Universitätsbibliothek im Jacob-und-Wilhelm-Grimm-Zentrum für eine Hybridlösung entschied, da es nicht möglich gewesen

wäre, bis zur Eröffnung alle Ausleihbestände mit Tags zu versehen [3, S. 592]. Insgesamt ist die Entwicklung zum Einsatz von RFID allerdings absolut positiv zu sehen, auch in Anbetracht künftiger logistischer Herausforderungen gerade in großen und verteilten Bibliothekssystemen.

Automatisierte Logistikkreisläufe im Bibliotheksbereich

Unter einer Logistikkette versteht man ganz allgemein gesprochen eine Reihe von Prozessen, die notwendig sind, ein Produkt vom Rohstoff bis zum Endverbraucher zu begleiten (Teil der Wertschöpfungskette) im engeren Sinne beschreibt eine Logistikkette den Weg eines Produkts von der Fertigung bis zur Auslieferung an den Kunden. Wichtig sind dabei die Prozessorientierung, also die Auffassung der Logistikkette als einen Prozess, der sich in mehrere Vorgänge aufteilt und die Kundenorientierung, das heißt die Unterordnung des Prozesses unter die Maxime des bestmöglichen Services für die Kundin oder den Kunden. Entsprechend der verbreiteten Auffassung von Logistikketten als Warenketten wurde im Zusammenhang mit RFID-Lösungen hier zumeist über einen denkbaren gemeinsamen Standard von Verlagen bzw. Druckereien und Bibliotheken nachgedacht.

Auch Bibliotheken haben aber spezifische Logistikketten, da sie sich von den meisten Unternehmen dadurch unterscheiden, dass sie ihre Materialien nicht endgültig an die Kundinnen und Kunden abgeben, sondern sie nur verleihen und – in der Regel – nach einiger Zeit zurückerhalten. Die Kette wird hier zu einem Kreislauf. Bott unterscheidet transportlogistische und – unter Rückgriff auf Ewert und Umstätter- informationslogistische Prozesse in Bibliotheken [vgl. 4, S.28]. Im Gegensatz zu Bott würde ich die informationslogistischen Prozesse nicht unbedingt an die transportlogistischen gekoppelt sehen, da die Information nicht immer als Kopie auf einem physischen Träger übergeben wird. Umgekehrt sind aber alle transportlogistischen Aufgaben in der Bibliothek auch informationslogistische und hierin liegt das Potential der RFID in den Logistikkreisläufen von Bibliotheken.

Automatisierung findet in diesem Kreislauf bisher zumeist als Insellösung statt. Schon seit Jahrzehnten wird in großen Bibliotheken der hausinterne Transport von einer Station im Magazin zur Leihstelle und zurück automatisiert, seit einigen Jahren werden zunehmend die Ausleihprozesse durch Selbstverbuchung automatisiert und das oben beschriebene Beispiel zeigt, das man beide Komponenten durch die Sortierung miteinander verbinden kann. Hier kommt dann auch schon – wenn auch nicht notwendigerweise – RFID zum Einsatz. Weitere Anwendungen sind allerdings denkbar, wenn man beginnt, die Logistikkette bzw. den Logistikkreislauf in Bibliotheken als System zu begreifen, das man insgesamt weitgehend automatisieren kann. Im Folgenden möchte ich stichwortartig einige aktuelle Themen im Bezug auf Automatisierung im Logistikkreislauf der Bibliotheken nennen und mögliche Verknüpfungspunkte andeuten.

Dies beginnt mit einfachen Erweiterungen des bestehenden Systems. Ein direkter Anschluss der Transportanlage an Sortierraum und Poststelle hätte eine wesentliche Reduzierung manueller Eingriffe in den Logistikkreislauf mit sich gebracht. So hätte man von dort direkt die richtigen Zielorte für Medien aus anderen Standorten realisieren können,

die Kisten hätte der Transportdienst nur noch mitnehmen brauchen. Dies ließ sich aufgrund der beschriebenen Gebäudegeometrie nicht realisieren. Wäre die Anlage schon im Gebäudeprogramm etwa über die Definition eines Logistikkreislaufs näher beschrieben worden, hätte sich das sicher in der Entwurfsplanung realisieren lassen. Andere Systeme, deren Einsatzmöglichkeit in Bibliotheken erst in den letzten Jahren wahrgenommen wurde, spielten bei den Planungen im Jacob-und-Wilhelm-Grimm-Zentrum verständlicherweise noch gar keine Rolle.

Mit der zunehmenden Nachfrage nach Arbeitsplätzen und der im Verhältnis dazu abnehmenden Nachfrage nach gedruckten Medien in Wissenschaftlichen Bibliotheken stellt sich die Frage nach dem Flächenverbrauch für die Lagerung der Medien immer dringender. Flächenverbrauch und Unterhaltskosten großer Magazine mit Festplatzlagerung stehen oft in einem problematischen Verhältnis zur Nutzung der Bestände, auch und gerade wenn die Bibliothek einen Archivauftrag zu erfüllen hat und wenig Material aussondern kann. In den Vereinigten Staaten gehen mehr und mehr Wissenschaftliche Bibliotheken und Bibliothekssysteme aus diesem Grund dazu über, Automated Storage and Retrieval Systems (ASRS) einzusetzen, die anstelle eines klassischen Magazins eine digital gesteuerte chaotische Lagerung vornehmen und in ihrer gängigen Form als Vertical-Lift-Moduls (VLM) nicht von Menschen bedient werden müssen. Die Vorteile in der Magazinierung sind hier ein wesentlich geringerer Flächenverbrauch, je nach Einstellung des Systems eine maximale Ausnutzung der zur Verfügung stehenden Kapazität und die Möglichkeit optimaler Lagerungsbedingungen, da die Umweltbedingungen im Magazin menschliche Bedürfnisse nicht berücksichtigen müssen. Darüber hinaus entfallen alle organisatorischen, also verwaltungszentrierten Vorgänge, die in einem Magazin mit Festplatzlagerung notwendig sind. Diese Systeme werden von Bibliothekarinnen und Bibliothekaren oft noch kritisch gesehen, weil ein befürchteter Computerausfall bei der chaotischen Lagerung zum Verlust der Standortnachweise sämtlicher Medien führen könne. Ähnliche Befürchtungen wurden aber auch schon gegen die Abschaffung der Zettelkataloge ins Feld geführt.

Da bestimmte ASRS mit gängigen Transportkisten arbeiten können, ist der Anschluss an ein Transportsystem naheliegend. Ein ASRS Nahbereichs-Magazin kann dann die Kiste mit dem gewünschten Medium im 24/7-Betrieb zeitnah bereitstellen, der Vorgang des Aushebens aus der Kiste müsste weiterhin manuell erfolgen, könnte aber von der Nutzerin bzw. dem Nutzer bei anschließender oder gleichzeitiger Verbuchung per RFID eigenständig erledigt werden. Die Rückgabe könnte sich ähnlich gestalten. Wenn eine Sortiermaschine die Medien nicht nach Standorten, sondern nach Formaten sortiert und die Kästen effizient und möglichst störungsfrei belädt, wäre eine vollautomatische Zuführung zurückgegebener Bücher ins ASRS eine logische Erweiterung des im Grimm-Zentrum eingesetzten Systems.

RFID-Insellösungen wie intelligente Regale oder Bücherschränke bzw. die Bereitstellung von vorgemerkten Medien lassen sich ebenfalls in einen automatisierten Logistikkreislauf integrieren. Vor allem die relativ einfache Detektion der Medien erlaubt es theoretisch, jedes Medium innerhalb des Logistikkreislaufes ständig zu identifizieren, auch wenn es sich nicht an seinem, von der Festplatzlagerung vorgegebenen Standort befindet.

Voraussetzung für eine wirtschaftlich vertretbare und effiziente Lösung ist aber immer, den Logistikkreislauf komplett zu analysieren und ggf. neu zu strukturieren. Entscheidend ist dabei zunächst vor der Automatisierung die Optimierung. Unnötige Vorgänge die sich etwa aus der klassischen Magazin- oder Leihstellenorganisation erhalten haben, für einen RFID-gestützten, kundenorientierten Kreislauf aber unnötig sind, sollte man dabei eliminieren. Insgesamt sollte der Kreislauf straffer werden, Bestellungen und Medien durch möglichst wenig Hände gehen, egal ob es sich um Freihandbestände, Magazinbestellungen, Vormerkungen oder Fernleihen handelt. Erst danach sollte die Überlegung stehen, was man RFID-gestützt automatisieren bzw. auf Selbstbedienung umstellen kann.

Fazit

Die Verknüpfung verschiedener automatisierter Vorgänge innerhalb des Logistikkreislaufs einer Bibliothek, wie sie im Jacob-und-Wilhelm-Grimm-Zentrum mit der Koppelung von Medienrückgabe, -Sortierung und –Transport realisiert wurde, ist ein erster sinnvoller Schritt in Richtung einer weitgehenden Automatisierung. Leider wurden im genannten Beispiel, wie generell im Bibliothekswesen, die einzelnen Vorgänge nicht als ein Logistikkreislauf gesehen, der mit dem Ausheben eines Mediums am Standort (sei es im Freihandbereich oder in einem Magazin) beginnt und mit dem Einstellen desselben Mediums nach einem oder auch mehreren Nutzungsvorgängen wieder endet. Vielmehr schlägt immer wieder die klassische Fokussierung auf die Verwaltung der Medien durch. Will man aber das Potential berührungs- und sichtkontaktfreier Identifikation von Medien, das die RFID-Technik bietet, jenseits von (verknüpften) Insellösungen innerhalb der Kreisläufe nutzen, ist die individuelle Analyse und Optimierung derselben unbedingt notwendig. Hier zeigt sich zunächst, welche Prozesse man gar nicht automatisieren muss, weil sie Rudimente einer Bibliotheksorganisation vor der EDV-Einführung sind oder weil sie nur einer Selbstvergewisserung dienen. In einem zweiten Schritt entwickelt man Verknüpfungen zwischen den definierten Prozessen und erkennt das Automatisierungspotential.

Jedes RFID-Projekt, das sich nicht nur als Insellösung zur Automatisierung bestimmter Vorgänge versteht und jedes (Um-)Bauprojekt im Bibliotheksbereich setzt – unabhängig von der Größe der Bibliothek – eine solche Analyse voraus. Dieser Aspekt ist bisher in der gängigen Literatur zum Bibliotheksbau und –Management aber auch zum RFID-Einsatz in Bibliotheken ein Desiderat und verdient es dringend, eingehender beschrieben und in der Praxis erprobt zu werden.

Literatur und Internetquellen

[1] Richter, A. (2009). Förder- und Sortiertechniken. In P. Hauke & K. U. Werner (Hrsg.), Bibliotheken bauen und ausstatten (S. 175-181). Bad Honnef: BOCK + HERRCHEN.

[2] Humboldt-Universität zu Berlin, Technische Abteilung (Hrsg.). (2004). Jacob und Wilhelm Grimm-Zentrum Berlin Mitte: Zentrale Universitätsbibliothek und Computer- und Medienservice; Offener Realisierungswettbewerb Ausschreibung. Berlin: Senatsverwaltung für Stadtentwicklung.

[3] Berghaus-Sprengel, Anke, Kühne, Tobias. (2009). Das RFID-Projekt an der Bibliothek der Humboldt-Universität zu Berlin – Stand und Perspektiven. Bibliotheksdienst, 43/6, 588-598.

[4] Bott, Anna. (2010). Informationslogistik an einer Hochschulbibliothek unter Berücksichtigung von Erfahrungen aus anderen Industriezweigen: Bachelor Thesis HAW Hamburg. Unveröffentlichtes Manuskript.

Wirtschaftlichkeit und Wirtschaftlichkeitsprüfung von RFID in Bibliotheken

Rainer Sprengel

Wirtschaftlichkeit ist ein zwingend zu beachtendes Gebot jeder Haushaltsführung der öffentlichen Hand. Doch was ist damit konkret gemeint? Und ist immer ein- und dasselbe gemeint? Bei näherer Betrachtung erkennt man schnell, dass es unterschiedliche und teilweise miteinander wenig kompatible Wirtschaftlichkeitspostulate gibt. Eine Bibliothek, die RFID einführen will, sieht sich unterschiedlichen Kontexten gegenüber, in denen sie die Frage, ob ein Einsatz von RFID »wirtschaftlich« ist, beantworten kann bzw. muss. Einige davon werden zunächst thematisiert. Im Anschluss wird das Tool WiBe vorgestellt, das es erlaubt, die Grunddaten und Argumente für die skizzierten unterschiedlichen Perspektiven in einem kontrollierten, anerkannten und rational gesteuertem Verfahren zu gewinnen.

Unterschiedliche Perspektiven auf Wirtschaftlichkeit

In diesem Abschnitt sollen vier Perspektiven kurz beleuchtet werden, aus denen das Thema der Wirtschaftlichkeit jeweils unterschiedliche Bedeutung gewinnt: Wirtschaftlichkeit aus der Perspektive interner Steuerung, Wirtschaftlichkeit aus der Perspektive des Unterhaltsträgers, Wirtschaftlichkeit aus der Perspektive eventueller Drittmittelgeber und schließlich Wirtschaftlichkeit aus der Perspektive des Vergaberechts.

Wirtschaftlichkeit aus der Perspektive interner Steuerung

Das Thema der Wirtschaftlichkeit aus der Perspektive interner Steuerung verknüpft den Horizont der Definition von eigenen Bibliothekszielen und Bibliotheksentwicklungsplänen mit der Frage nach einer nachhaltigen und optimalen Verwendung verfügbarer Ressourcen, angefangen von Gebäuden über Personal bis hin zu verfügbaren Geldbeträgen. Eine Bibliothek, die lediglich fünfzig Stunden in der Woche für das Publikum geöffnet hat, nutzt die Ressource Gebäude in ökonomischer Sicht suboptimal, denn sie hat 118 Stunden in der Woche geschlossen. Da für die meisten Bibliotheken heute gilt, dass sie über ihre Nutzung durch Benutzer gerechtfertigt werden, bedeutet das, dass die gesamten Gebäudekosten auf die fünfzig Öffnungsstunden kalkulatorisch umgelegt werden müssen, wenn man darstellen will, wie teuer die erbrachte Leistung Bibliothek im konkreten Fall ist. Gelingt es durch die Einführung einer Technik wie RFID, die Öffnungszeiten mit dem vorhandenen Personal zu verdoppeln, halbiert sich dieser Preis für die angebotene Leistung. Wenn diese dann durch eine erhöhte Nachfrage auch angenommen wird, hat man das Äquivalent zu dem Preis, der ansonsten auf Märkten das Resultat des Spiels von Angebot und Nachfrage ist. Anders gesagt: obgleich möglicherweise zusätzliche Betriebskosten hinzukommen, steht die Bibliothek im Sinne einer Kosten-Leistungs-Relation sparsamer und effizienter da.

Bei näherer Betrachtung ist diese Perspektive besonders komplex, da in ihr aus interner Sicht, die Bibliothek als System mit all ihren Verzweigungen, externen und internen Zwängen, Traditionen und Absurditäten thematisiert wird. Diese Thematisierung führt zu einer Menge an Wenn-Dann-Beziehungen, die in ökonomischen Äquivalenten in Form von Geldeinheiten kalkuliert werden müssen. Im vorherigen Absatz bestand diese Wenn-Dann-Beziehung darin, dass die Verdopplung der Öffnungszeit mit Hilfe der Technik gelinge, wenn kein Personal abgebaut wird. Da letzteres aber häufig im Zuge solcher Investitionsmaßnahmen von Unterhaltsträgern im Namen vermeintlicher Sparsamkeit als Gegenleistung erwartet wird, muss man dann genau schauen, ab welchem Punkt die Investition kontraproduktiv wird. Sparen kann einer sparsamen Mittelverwendung dann widersprechen, wenn die bisher erbrachte Dienstleistung nicht verbessert und nicht billiger gemacht werden kann, dafür aber einen neue Abhängigkeit gegenüber einem externen, profitorientierten Anbieter entsteht. In solch einem Fall sollte man die Finger von einer Investition in RFID lassen.

Grundlage der Prüfung von Wirtschaftlichkeit aus der Perspektive interner Steuerung ist also die Definition von (ambitionierten) Bibliothekszielen und einer Modernisierungsstrategie im Rahmen einer Bibliotheksentwicklungsplanung. Solche längerfristig ausgerichteten Überlegungen stellen erst den Kompass dar, der es ermöglicht zu entscheiden, ob, wo und wie die Einführung von RFID in einer Bibliothek zielführend ist: Erst die Definition der Ziele, dann die Festlegung der geeigneten technischen Mittel.

Im Rahmen der Prüfung der geeigneten technischen Mittel, um die avisierten Ziele zu erreichen, erhält eine Wirtschaftlichkeitsprüfung erst ihre richtige Funktion. Mit ihr prüft man zweierlei kritisch ab.

Erstens geht es um die Frage, ob das für gut erachtete Szenario der Einführung überhaupt in Einklang zu bringen ist mit verfügbaren oder erwartbaren Haushaltsmitteln. Nur wenn man sich genug RFID leisten kann, um die avisierten Ziele zu erreichen, macht eine solche Investition Sinn – ansonsten wird es leicht zu herausgeworfenem Geld.

Zweitens aber kann man mit einer Wirtschaftlichkeitsprüfung insbesondere auch eine mittelfristige Betrachtung der Betriebskosten eines neuen Systems im Verhältnis zum erwarteten und wirtschaftlich zu beziffernden Nutzen vornehmen. Das ermöglicht insbesondere auch die Festlegung von Erfolgsindikatoren, die es später erlauben festzustellen, ob die Ziele tatsächlich erreicht werden konnten.

Eine Öffentliche Bibliothek definierte z. B., dass sie
1. die Öffnungszeiten um ca. 8 %,
2. die frühkindliche Leseförderung,
3. die Zusammenarbeit mit Kitas und Schulen
4. die Arbeit mit Jugendlichenverbessern und innovativ ausbauen will.

Um die nötige Zeit für ihr Personal zu erwirtschaften, soll das vorhandene Personal von repetitiven Vorgängen im Ausleihbereich durch RFID entlastet werden. In diesen Rahmen werden auch Ziele der Personalentwicklung und der Fortbildung eingeordnet. Bei einer Wirtschaftlichkeitsprüfung dieses Einführungsszenarios reicht es daher nicht,

lediglich die Kosten für RFID-Geräte und deren Betrieb zu kalkulieren. Man wird etwa prüfen müssen, ob das vorhandene Personal tatsächlich frei gewordene Zeit für die qualitativen Ziele im Bereich der frühkindlichen Leseförderung nutzen kann. Braucht es dafür besondere Schulungen und Fortbildungen, sollten die Kosten hierfür bei einer Wirtschaftlichkeitsprüfung berücksichtigt werden. Ebenso gilt dies, wenn sich dadurch Stellenprofile so ändern, dass eine Höhergruppierung rechtlich geboten ist. Wer A sagt, muss auch B sagen. Dieser Leitsatz aus Hänsel und Gretel gilt für jede solide Wirtschaftlichkeitsprüfung. Abgesehen vom Umfang der Öffnungszeiten, die leicht zu messen sind, ist es auch eine besondere Aufgabe, Indikatoren festzulegen, um die Verbesserung der qualitativen Dienstleistungen gegenüber Kindern und Jugendlichen zu messen. Hat man z. B. bisher 40 % der Kitas erreicht, kann man als Ziel 50 % formulieren, wenn dies die erwarteten Zeitspareffekte zulassen.

Eine Wissenschaftliche Bibliothek definierte demgegenüber als Ziele:
1. Konzentration der Standorte
2. Drastische Erweiterung der Öffnungszeiten in Richtung 24/7
3. Integration der Kassenfunktion (Gebühren) in die Selbstverbuchung
4. Verringerung der Buchmedienentführung um 10 %.

Erkennbar liegt der Fokus der wissenschaftlichen Bibliothek in diesem Fall auf einer Optimierung von Verwaltungsverfahren im Kundenkontakt, wobei entstehende Zeitressourcen für eine drastische Verlängerung der Öffnungszeiten verplant werden. Die hier zielführenden Aspekte scheinen leichter messbar zu sein. Für die Personalentwicklung kann man in diesem Szenario darüber nachdenken, ob es überhaupt einer Berücksichtigung von Kosten für Fortbildungen bedarf. Möglicherweise führt das hier gewählte Zielsystem auch eher zu einer mittelfristigen Abwertung der Besoldungsgruppen bzw. zu einem vermehrten Einsatz von nicht bibliothekarischem Wachpersonal oder studentischen Hilfskräften.

Der Vergleich zwischen der wissenschaftlichen und der öffentlichen Bibliothek unterstreicht noch einmal, wie wichtig die Zielformulierung aus der Innenperspektive im Rahmen der Wirtschaftlichkeitsprüfung ist. Erst durch diese wird festgelegt, was für Faktoren berücksichtigt werden müssen, um die mit einer konkreten RFID-Einführung verbundenen Kosten- und Nutzenaspekte zu identifizieren, die kalkuliert werden müssen, um die Frage danach, ob diese Einführung wirtschaftlich ist, beantworten zu können.

Je solider man auf dieser Ebene der vorbereitenden Wirtschaftlichkeitsprüfung arbeitet, desto besser sichert man sich auch ab, wenn sich im Verlaufe solcher mehrjährigen Projekte manche Dinge anders entwickeln. Wenn z. B. der Zuwendungsgeber überraschend die Fortbildungsmittel streicht, die man für die Verwirklichung der Projektziele benötigte, kann man gegenüber einer Prüfinstitution (Rechnungshof, Öffentlichkeit) zumindest darstellen, wer die Schuld daran hat, dass Steuergeld suboptimal oder gar unwirtschaftlich eingesetzt worden ist.

Wirtschaftlichkeit aus der Perspektive des Unterhaltsträgers

Aus der Perspektive des Unterhaltsträgers ist RFID in der Bibliothek zunächst einmal eine neue Ausgabenposition, die er im Hinblick auf die Einführung und den Dauerbetrieb als Kostenfaktor beziffert wissen will. Ungeachtet aller Verwaltungsreformen, geht die Frage nach einer Ausgabenbezifferung einher mit derjenigen nach der Darstellung von Einnahmen, mit denen diese Ausgaben finanziert werden sollen. Die Unterscheidung von Investition und Betrieb hat dabei für Unterhaltsträger lediglich den Effekt, dass auf unterschiedliche Posten im Haushalt zugegriffen werden kann. Eine Beachtung des Zusammenhangs von Investition und Ertrag findet dagegen in der Regel nicht statt.

Für Bibliotheken ist in der Praxis mit dieser Einnahmen-Ausgaben-Logik die Anforderung verbunden, Dauerbetrieb oder auch Investitionen durch Einsparen von Haushaltsmitteln an anderer Stelle gegen zu finanzieren.

Das Problem dieser Perspektive besteht darin, dass eine Einnahmen-Ausgaben-Logik keinen Platz für Wirtschaftlichkeitsargumente bietet. Die Bemühungen, über Kosten-Leistungs-Rechnungen und andere Instrumente die Grundlage dafür in öffentlichen Verwaltungen einzuführen, sind in der Fläche partiell und unvollständig geblieben – und selbst da, wo sie für interne Steuerungsprozesse auf Verwaltungsebene eingesetzt werden, lässt sich zeigen, dass bei vielen Entscheidern, etwa im politischen Raum, die Frage nach Ausgaben und deren konkreter Gegenfinanzierung (Drittmittel, Personalstellen usw.) primär ist.

Überlagert wird diese Perspektive bei Entscheidern allerdings durch Erwägungen ganz anderer Natur, die teilweise in Gefilde des »Das will ich auch in meiner Bibliothek haben« führen. Der Besuch einer gut laufenden RFID-Installation kann hier entsprechende Bedenken gegen vorgelegte Kostenrechnungen bei Seite schieben. Tatsächlich kann man bei mehreren Entscheidungsprozessen für RFID rekonstruieren, dass es nicht der Nachweis irgendeiner Wirtschaftlichkeit war, die die Entscheider auf der Seite des Unterhaltsträgers zu ihrer Zustimmung gebracht haben.

Die Darstellung von Wirtschaftlichkeit gegenüber dem Unterhaltsträger ist insofern zumindest teilweise strategischer Natur. Gleichwohl behält deren Solidität und Seriosität eine gewisse Bedeutung, da der Unterhaltsträger selbst wiederum kontrolliert wird, etwa durch Rechnungshöfe und Öffentlichkeit. Insofern hat auch der Unterhaltsträger ein strategisches Verhältnis zu einer Wirtschaftlichkeitsberechnung: Wenn sie aus der Schublade geholt werden muss, will der Unterhaltsträger auf der sicheren Seite sein, dass die einmal getroffene Entscheidung das Gebot der Wirtschaftlichkeit und Sparsamkeit öffentlicher Haushaltsführung nach bestem Wissen und Gewissen beachtet hat.

Wirtschaftlichkeit aus der Perspektive eventueller Drittmittelgeber

Gerade auch im investiven Bereich haben sich mittlerweile Mischfinanzierungen etabliert, bei denen sogenannte Drittmittelgeber auftreten. Manchmal handelt es sich um private Förderer wie Fördervereine, Stiftungen oder sponsernde Unternehmen, wobei letzteres schnell in Konflikt mit Antikorruptionsrichtlinien kommen kann. Für solche

Akteure haben Wirtschaftlichkeitsbetrachtungen im Sinn der öffentlichen Hand keine echte Bedeutung. Diese Akteure wollen ihr Geld sinnvoll ausgegeben wissen, wobei sie sich eher wenig für die Finanzierung notwendiger Betriebskosten begeistern lassen, als vielmehr für interessante und hübsche Projekte.

Für Infrastruktureinrichtungen wie es Bibliotheken sind, treten deshalb häufiger andere Drittmittelgeber auf, hinter denen sich selbst wieder die öffentliche Hand verbirgt. Die heißen dann Strukturfonds oder Konjunkturprogramm. Obgleich immer Steuergeld (oder im Namen des Steuerzahlers geliehenes Geld) ausgegeben wird, verkehrt dabei die öffentliche Hand mit sich selbst in Form von Antragsteller und außerordentlichem Zuwendungsgeber. Da es sich um Gelder der öffentlichen Hand handelt, unterliegt es naturgemäß den schon erwähnten Geboten der sparsamen und wirtschaftlichen Mittelverwendung, wobei sich die Kriterien dafür aus den jeweiligen Fonds- und Programmzielen herleiten.

Damit entsteht für eine Bibliothek, die hieraus Gelder für eine RFID-Einführung erhält das Problem, das eigene Zielsystem möglichst reibungsfrei in dieses externe Zielsystem abzubilden. Das gelingt unproblematisch, wenn die für ein Programm verantwortlichen Funktionsträger sich als Sachwalter einer Verwaltungsfunktion verstehen.

Unabhängig von der Wahrnehmung der eigenen Rolle, hat dieser seltsame Verkehr der öffentlichen Hand mit sich selbst einen unmittelbaren wirtschaftlichen Effekt: es kostet Zeit und damit Geld für Antragstellung und zusätzliche Mittelverwendungsprüfungen. Zumindest in Form der Kalkulation eines entsprechenden zusätzlichen Personalaufwandes sollte die Art der Finanzierung kalkulatorisch in eine Wirtschaftlichkeitsbetrachtung eingehen.

Wirtschaftlichkeit aus der Perspektive des Vergaberechts

Die Perspektive des Vergaberechts auf das Gebot der sparsamen Mittelverwendung ist paradox. Es soll zwar eine sparsame Beschaffung von Dingen und Dienstleistungen ermöglichen, indem es insbesondere auch Vorteilsnahmen und Bequemlichkeit unterbindet. Zugleich jedoch steht es auch im Dienst einer allgemeinen Regulierungsfunktion des Staates. Dies drückt sich darin aus, dass das Vergaberecht den Staat selbst daran hindert, seine in Teilen bestehende Monopolstellung gegenüber Anbietern auszunutzen. Vergaberecht zielt insofern nicht nur darauf ab, einen fairen Wettbewerb zu ermöglichen, der nicht durch Korruption oder Faulheit verfälscht wird, sondern intendiert ebenso, dass die Anbieter einen fairen Preis für ihre Dienstleistungen und Güter erhalten. Für die Praxis im RFID-Bereich ergeben sich hieraus manche Probleme, die aber an anderer Stelle thematisiert werden (vgl. Beitrag zum Thema Ausschreibungen).

Wie auch immer: Bei nachhaltig mit Kosten verbundenen RFID-Investitionen ist die Darstellung der Wirtschaftlichkeit vergaberechtlich zwingend notwendig.

Prüfung der monetären Rentabilität

Die bisherige Skizzierung unterschiedlicher Perspektiven auf das Thema Wirtschaftlichkeit wirft das Problem auf, wie man konkrete Wirtschaftlichkeitsbetrachtungen so durchführt, dass man in unterschiedlichen Kontexten Auskunft darüber geben kann, ob sich z. B. eine Einführung von RFID im Benutzungsbereich rechnet, also die Investition und die sich an die Investition anschließenden Betriebsausgaben rentabel sind. Am weitesten kommt man, wenn man die Grunddaten und Argumente für die skizzierten unterschiedlichen Perspektiven in einem kontrollierten, anerkannten und rational gesteuertem Verfahren gewinnt. Da für die meisten Bibliotheken öffentliche Finanzierungskontexte vorherrschend sind, ist es sinnvoll, auf Tools zurück zu greifen, die für die Bedürfnisse und Besonderheiten der öffentlichen Hand gemacht sind.

Mit dem Programm WiBe liegt ein softwaregestütztes Tool vor, das seit 1992 in der Bundesverwaltung im Einsatz ist und mehrfach aktualisiert wurde.[1] Dazu gehört das umfängliche Fachkonzept »Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT«, verantwortet von der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) beim Bundesministerium des Innern. Es ist ein für alle Anwender im Öffentlichen Dienst kostenlos erhältliches Tool, das sich durch leichte Bedienbarkeit und Anwenderfreundlichkeit auszeichnet. Es ist inhaltlich für alle Wirtschaftlichkeitsbetrachtungen geeignet, die einen wesentlichen technologischen Kern haben, und es berücksichtigt die Vorgaben der Bundeshaushaltsordnung. In Berlin gehört der Einsatz von WiBe zudem zum Mechanismus der Beteiligung des Hauptpersonalrates, um das Thema der Wirtschaftlichkeit bei beteiligungspflichtigen Maßnahmen darzustellen. Es ist also in einem sehr weiten Sinne ein anerkanntes Verfahren.

Das Tool verlangt eine vollständige Erfassung aller unmittelbaren Kosten- und Nutzenaspekte in EURO-Geldbeträgen inkl. MwSt. Dabei werden die haushaltswirksamen und die nicht haushaltswirksamen Kosten- und Nutzenbeträge differenziert aufgeführt. Nutzen und Kosten werden im Vergleich zum bestehenden Altsystem ermittelt. Wenn man ein Ausleihsystem auf der Basis von Barcodes durch eines von RFID ersetzt, werden die entsprechenden Kosten, die für Ausleihe, Rückgabe und Sicherung bisher entstehen mit den künftigen Kosten verrechnet.

Erstinvestition und Dauerbetrieb werden unabhängig voneinander erfasst und können unabhängig voneinander dargestellt werden. Die Tabellen, in die die Beträge eingetragen werden, erlauben eine klare Darstellung einmaliger Kosten/Nutzeneffekte sowie wiederholter Kosten-/Nutzeneffekte, zugeordnet nach den anfallenden Jahren. Im Rahmen der Wirtschaftlichkeitsbetrachtung werden diese miteinander verrechnet.

Dabei wird die Kapitalwertmethode angewendet, d. h. der Zeitpunkt der Ausgabe bzw. Einnahme mit einem Zinssatz bewertet. Die Bewertung wurde in anderen Bibliotheken mit einem Zinssatz von 4 % durchgeführt. Der Prozentsatz sollte sich dabei an einem langjährigen Mittel orientieren, was man am Kapitalmarkt bei konservativer Anlage als

1 http://www.cio.bund.de/cln_155/DE/IT-Methoden/WiBE/wibe_node.html

Wertsteigerung hätte erzielen können. Dieses Verfahren ist einer reinen Einnahme-/Ausgabenbetrachtung überlegen, da letztere nicht in der Lage ist, angemessen das Verhältnis zwischen Investitionskosten und späterem Ertrag darzustellen. Dieser spätere Ertrag muss deutlich höher als die Investition ausfallen, um in einem monetären Sinn als rentabel gelten zu können.

Die Berechnungszeit ist zwar prinzipiell frei wählbar, muss sich aber gemäß dem Fachkonzept an den Systemeigenschaften orientieren. Bei reinen IT-Maßnahmen wird man eher vier Jahre wählen, weil spätestens dann die Hardware so veraltet ist, dass sie ausgetauscht werden muss. Bei RFID-Installationen kann der gewählte Zeitraum deutlich länger bis zehn Jahre gefasst werden, zumal die angemessene Berücksichtigung der laufenden Betriebskosten Pauschalen für Geräteersatz und Softwareupdates erlaubt.

Das Fachkonzept unterstützt durch eine klare Untergliederung die Ermittlung aller relevanten haushaltswirksamen und nicht haushaltswirksamen Positionen. Grundsätzlich sind ermittelte Marktpreise anzusetzen. Hierfür gibt es z. B. Marktübersichten der Anwendergruppe RFID im Deutschen Bibliotheksverband, die auf durchgeführten Ausschreibungen beruhen.

Wenn diese nicht existieren, sind entsprechende Kostensätze anzuwenden oder es werden Prozentsätze empfohlen. Dieses Verfahren wurde im Rahmen der Wirtschaftlichkeitsbetrachtung einer RFID-Einführung im VÖBB in Berlin erfolgreich durchgeführt.

Nicht dargestellt werden häufig in Kostenkalkulationen die nicht haushaltswirksamen Kosten- und Nutzeneffekte. Diese sind aber für eine Wirtschaftlichkeitsrechnung nach WiBe zwingend zu berücksichtigen. Erfahrungsgemäß macht dies vielen Akteuren der öffentlichen Hand große Probleme, da sie es in der Praxis gewohnt sind, nur über in einem Haushaltsjahr frei verfügbare Haushaltsmittel nachzudenken. Im Rahmen von WiBe sind haushaltswirksame und nicht haushaltswirksame Beträge vollkommen gleichrangig, und das zu Recht, denn beide werden real aus Steuermitteln finanziert.

Tatsächlich wird man feststellen, dass der jeweils kalkulierbare Nutzen nicht haushaltswirksamer Natur ist. Der Spareffekt bei fest angestelltem Personal im Ausleihbereich kann unabhängig von den Projektzielen schon deshalb nicht unmittelbar haushaltswirksam gemacht werden, weil dies nur durch Entlassungen ginge. Das obige Beispiel der besseren Nutzung eines Gebäudes durch längere Öffnungszeiten ist als Nutzen ein rein nicht haushaltswirksamer Effekt – bei genauer Erfassung wird man zudem erhöhte Kosten für den Gebäudebetrieb, etwa für Heizung, Licht oder Reinigung berücksichtigen müssen. Mit anderen Worten: der nicht haushaltswirksame Nutzen kann zugleich weitere höhere haushaltswirksame Kosten nach sich ziehen. Gerade deshalb ist es wichtig die Wenn-Dann-Kausalitäten möglichst genau zu erfassen, denn natürlich kann es passieren, dass die mögliche bessere Gebäudenutzung schlicht daran scheitert, dass dem Zuwendungsgeber das Geld für Heizung und Licht ausgeht.

Im Rahmen einer Wirtschaftlichkeitsbetrachtung geht die Liste der zu beziffernden Kosten- und Nutzenfaktoren also deutlich über eine Beschreibung dessen hinaus, was man unmittelbar kaufen will.

Eine Liste der Kostenfaktoren für eine RFID-Einführung kann entsprechend umfassen:

1. Haushaltswirksame Investitionskosten für die Beschaffung von Tags, Konvertierstationen, Selbstverbucher, Rückgabegeräte, Software oder Sicherungsgates
2. Haushaltswirksame Betriebskosten für die laufende Beschaffung von Tags, die Pflege und Aktualisierung von Software, von Selbstverbuchern, Rückgabegeräten oder Sicherungsgates, ggf. in Form von Pauschalen gemäß der WiBe-Anleitung
3. Haushaltswirksame Personalkosten insbesondere für extra eingestellte Mitarbeiter
4. Nicht haushaltswirksame Personalkosten insbesondere für das Einführungsmanagement durch die Direktion einer Bibliothek, für Ausschreibungen, Personalversammlungen u. ä. sowie für die Ausstattung der Medien mit Tags und die Konvertierung aller Medien durch eigenes vorhandenes Personal
   - 4.1. Reisekosten zum Beispiel für die Teilnahme an Gremien oder die Besichtigung existierender Installationen und den Erfahrungsaustausch
   - 4.2. Haushaltswirksame oder nicht haushaltswirksame Mittel für Schulungen und Aktivitäten im Bereich des Veränderungsmanagements. (die StB München hat in diesem Bereich 330 € pro Personalstelle eingesetzt)
   - 4.3. Haushaltswirksame oder nicht haushaltswirksame Mittel für Schulungen und Aktivitäten im Bereich von Schulungen, um die Projektziele zu erreichen
   - 4.4. Haushaltswirksame Kosten für Höhergruppierungen im Zuge eines höheren Anforderungsprofils an die bibliothekarische Tätigkeit

Diese Liste kann länger oder kürzer werden, je nachdem, was man mit einer RFID-Einführung erreichen will. Ebenso können die eingesetzten Beträge Pauschalen oder ermittelte Markt-Werte sein. Für den Bereich der Kalkulation der nicht haushaltswirksamen Personalmittel wird man in der Regel auf entsprechende Tabellen des Zuwendungsgebers zurückgreifen.

Eine Liste des Nutzens einer RFID-Einführung findet vor allem im Kontext des Betriebs Berücksichtigung. Diese Liste kann zum Beispiel umfassen:

1. Haushaltswirksamer Wegfall der Kosten für bisherige Sicherungssysteme
2. (Nicht) haushaltswirksamer Wegfall von Personalkosten für die Durchführung von Ausleihvorgängen
3. Nicht haushaltswirksamer Wegfall von Kosten für die Zurüstung von Medien für spezielle Safersysteme
4. Nicht haushaltswirksame Verbesserung des Nutzungsgrades eines Gebäudes

Zu überlegen ist dabei, ob man auf der Nutzenseite lediglich vom Status Quo ausgeht, d. h. keine Leistungssteigerung des Systems durch erhöhte Nachfrage kalkulatorisch berücksichtigt, obwohl Erfahrungen aus anderen Städten zeigen, dass diese als Folge einer verbesserten Dienstleistung nach der Einführung von RFID eintreten wird (z. B. durch verbesserte Öffnungszeiten und bessere Beratung) – oder ob man solche erwarteten Effekte einpreist.

Wenn man alle Kosten und Nutzenfaktoren ermittelt und in die Tabellen eingegeben hat, sieht man als ein zentrales Ergebnis die Darstellung einer monetären Rentabilität in der Form: +107.378,66 € oder aber -127.884,22 €. Handelt es sich im Ergebnis um einen

positiven Wert, besagt dies, dass das geprüfte Projekt in monetärer Hinsicht rentabel, d. h. gegenüber dem Altsystem eine sparsamere Haushaltsführung darstellt. Der Ausdruck meint, dass die öffentliche Hand in der Verrechnung aller Positionen unter dem Strich über 100.000 € weniger aufwendet als ohne die geplante Maßnahme. Ist der Wert mit einem Minus versehen ist das Gegenteil der Fall.

Damit hängt natürlich alles an der Güte der eingegebenen Werte. Da man z. B. vor einem Zuschlag nach einer Ausschreibung gar nicht genau wissen kann, wie teuer oder billig man etwa die RFID-Technik tatsächlich erhält, sind die eingegebenen Werte unsicher. Problematisch ist daran vor allem, dass die Werte unterschiedlich sicher sind. Manche Marktentwicklung ist präzise vorhersehbar, etwa bei den Preisen für Tags. Bei anderen Aspekten hingegen kann sich die Konfiguration des Bibliotheksmanagementsystems preistreibend auswirken, wobei die Höhe der hier anzusetzenden Anpassungskosten sich je nach ausgewähltem RFID-Anbieter unterscheiden können. Deshalb ist es sinnvoll, auf der Seite der Kosten eher dem höheren Preis, auf der Seite des Nutzens eher dem geringeren Nutzen Vorrang zu gewähren.

Zudem stellt WiBe u. a. auch dar, wie signifikant der gewonnene Wert ist, denn es ist leicht nachzuvollziehen, dass ein Gewinn oder Verlust von 100.000 € hoch signifikant ist, wenn im Projekt Kosten und Nutzen in Höhe von 1 Mio. € verrechnet werden, aber deutlich weniger aussagekräftig ist, wenn man dabei 100 Mio. € verrechnet hat.

Nur und ausschließlich, wenn man einen positiven Ertrag im Ergebnis hat, kann man zu der Aussage kommen, dass das geplante Projekt dem Gebot der sparsamen und wirtschaftlichen Mittelverwendung nicht nur genügt, sondern zu seiner Beachtung sogar angezeigt ist. Ist der Betrag negativ, verstößt das Projekt hingegen dagegen. Wenn die zentrale Vorgabe für ein RFID-Projekt ein im rein monetären Sinn sparsamerer Betrieb sein sollte, wäre das Projekt damit gestoppt. Ansonsten jedoch kann man eine erweiterte Wirtschaftlichkeitsbetrachtung in Form einer Nutzwertanalyse durchführen.

Erweiterte Wirtschaftlichkeitsbetrachtung

WiBe beschränkt sich nämlich nicht auf eine Betrachtung der monetären Rentabilität, sondern sieht ebenso eine Nutzwertanalyse vor. Die Nutzwertanalyse ist notwendig und zentral, weil die öffentliche Hand kein gewinnorientierter, sondern ein aufgabenorientierter Betrieb ist. Für diese Nutzwertanalyse stehen drei Module, die ein Frage- und Punktebewertungsraster vorgeben, mit folgenden Inhalten zur Verfügung:

1. Modul »WiBe-D« (Dringlichkeitskriterien): Mit WiBe-D soll ermittelt werden, wie dringlich die Einführung eines neuen Systems bzw. die Ersetzung eines vorhandenen Altsystems ist. Dabei kann es Kriterien geben, die die Einführung eines Neusystems erzwingen, wenn sich zum Beispiel eine veränderte Rechtslage ergeben hat, der das vorhandene System nicht genügt.
2. Modul »WiBe-Q« (Qualitativ-strategische Kriterien): Mit Wibe-Q wird es möglich, eine qualitativ-strategische Wirkung einer beabsichtigten Einführung eines neuen System zu messen, bei der behördeninterne Qualitätsverbesserungen bzw. die Wirkung auf Mitarbeiter, wie z. B. Verbesserungen im Bereich der Ergonomie, erfasst werden.

3. Modul »WiBe-E« (Externe Effekte): Mit Wibe-E kann man externe Effekte in der Wirtschaftlichkeitsbetrachtung berücksichtigen, wie z. B. ein verbesserter Service für Kunden.

Aufgabe und Problem dieses Teils der Wirtschaftlichkeitsbetrachtung ist die Tatsache, dass es sich hierbei nicht um monetäre Bewertungen handelt. Daher ist es ein Vorzug, dass die Module inhaltlich durch Fragen vorstrukturiert sind und ein Bewertungsraster vorgegeben ist. Dieses Bewertungsraster weist jedem Fragenkomplex ein Bewertungsschema von 0-10 Punkten zu. Bei der Auswertung greift ein vorgegebenes Gewichtungsraster mit Multiplikationsfaktoren von 2 bis 25.

Man sollte auf eine Modifikation des Bewertungsrasters und des Gewichtungsschemas verzichten, um subjektive Aspekte bei der Bewertung zu beschränken.

Das Fachkonzept WiBe sieht die Durchführung einer erweiterten Wirtschaftlichkeitsbetrachtung nur dann zwingend vor, wenn eine monetäre Rentabilität nicht gegeben ist. In diesem Fall soll eine Nutzwertanalyse zeigen, ob es andere Gründe gibt, die eine Maßnahme rechtfertigen und welcher Art diese Gründe sind.

Gleichwohl empfiehlt das Fachkonzept auch dann die Durchführung der erweiterten Wirtschaftlichkeitsbetrachtung, wenn diese nicht zwingend ist. Tatsächlich misst diese den erwarteten Nutzwert. Da es sich um ein qualitatives Verfahren handelt, gehen in dieses auch die subjektiven Wertungen ein, auf welchen Wegen die weitere Arbeit voranschreiten soll und ob dabei die betrachtete Maßnahme einen Beitrag (Nutzen) liefert oder eher nicht. *Genauso wie es Maßnahmen gibt, die monetär nicht rentabel, aber qualitativ von hohem Nutzen sein können, kann es auch monetär rentable Maßnahmen geben, die ohne Nutzen sind.*

Ausgehend von dem zur Verfügung stehenden Tool mit seiner am IT-Bereich orientierten Fragebatterie, wurde mittlerweile ein RFID-orientiertes Design erarbeitet und in der Praxis angewendet. So haben 2007 Amtsleitungen im VÖBB dieses dann bearbeitet[2], auch im Projekt der Bibliothek der Humboldt-Universität wurde 2009 entsprechend verfahren[3]. Die publizierten Ergebnisse seien hier als Illustration kurz diskutiert.

Die maximal erreichbare gewichtete Punktzahl jeden einzelnen Moduls beträgt 100. Um die maximale Punktzahl zu erreichen, wobei müssten allerdings gleich mehrere Kriterien in einer Weise gewertet werden, dass schon jede einzelne dieser Wertungen eine Maßnahme erzwingen würde. Der folgende Überblick zeigt die Ergebnisse für die drei Module, sortiert nach den Werten aus dem Modul-Q, Qualitativ-strategische Aspekte. Sie stammen aus durchgeführten Wertungen innerhalb des Berliner Bibliothekswesens. Vertreten sind eine Universitätsbibliothek, dann die Landesbibliothek sowie Öffentliche Bibliotheken aus Berliner Bezirken.

---

2 Vgl. Rainer Sprengel: RFID-Prüfgutachten. Zur Einsatzmöglichkeit von RFID in den Öffentlichen Bibliotheken Berlins. Berlin 2007. Quelle: http://www.bibliotheksportal.de/hauptmenue/themen/rfid/materialien-downloads/publikationen-gutachten/

3 Vgl. Anke Berghaus-Sprengel, Tobias Kühne: Das RFID-Projekt an der Bibliothek der Humboldt-Universität zu Berlin – Stand und Perspektiven, in: Bibliotheksdienst 43. Jg. (2009), H. 6, S. 588-598

Bibliothekssystem	Qualitativ-strategische Aspekte	Dringlichkeit	Externe Effekte
Humboldt-Universität Berlin (2009)	73	71	63
Stiftung Zentral- und Landesbibliothek Berlin (2007)	49	23	49
Bezirk Neukölln Berlin (2007)	63	35	64
Bezirk Pankow Berlin (2007)	60	35	30
Bezirk Marzahn-Hellersdorf Berlin (2007)	58	54	48
Bezirk Charlottenburg-Wilmersdorf Berlin (2007)	27	22	23
Bezirk Lichtenberg Berlin (2007)	19	14	18

Zusammengefasst kann man die Werte so interpretieren:

1. Das bibliothekarische Führungspersonal in den jeweiligen Einrichtungen hat sehr unterschiedliche Vorstellungen davon, was es glaubt, mit RFID erreichen zu können oder auch nicht erreichen zu können.
2. Unterschieden werden kann zwischen solchen Institutionen, die über alle Felder hinweg gleichmäßig hohe/niedrige Erwartungen an RFID hatten (z. B. HU-Bibliothek als Beispiel für hoch, Lichtenberg für niedrig), und solchen Institutionen, bei denen ein Wertungsbereich abfällt/heraussticht.

Damit schließt sich der anfangs aufgemachte Kreis zwischen der Formulierung von Zielstellungen für eine RFID-Einführung und der Prüfung der Wirtschaftlichkeit solch einer Einführung. Die Prüfung der Wirtschaftlichkeit ist insofern primär ein wichtiges Mittel zur Klärung der verfolgten Projektziele und damit der internen Projektsteuerung und gibt doch zugleich sekundär die Grundlage für eine Absicherung des Projekts und der sie verantwortenden Personen gegenüber den mitunter wechselhaften Einfällen, Eingriffen und Kontrollen von Unterhaltsträgern, Zuwendungsgebern und Prüfinstitutionen ab.

Richtig verstanden und gemacht ist die Prüfung der Wirtschaftlichkeit also keine mühevolle und zusätzliche Arbeit für die Schublade, sondern ein Instrument für eine intelligente und finanzierbare Bibliotheksentwicklung.

Literatur und Internetquellen

[1] Die Beauftragte der Bundesregierung für Informationstechnik. (2011). Wirtschaftlichkeitsbetrachtungen. http://www.cio.bund.de/cln_155/DE/IT-Methoden/WiBE/wibe_node.html

[2] Sprengel, Rainer. (2007). RFID-Prüfgutachten. Zur Einsatzmöglichkeit von RFID in den Öffentlichen Bibliotheken Berlins. Berlin. http://www.bibliotheksportal.de/hauptmenue/themen/rfid/materialien-downloads/publikationen-gutachten/

[3] Berghaus-Sprengel, Anke; Kühne, Tobias. Das RFID-Projekt an der Bibliothek der Humboldt-Universität zu Berlin – Stand und Perspektiven, In: Bibliotheksdienst 43 (2009), H. 6, S. 588-598

Die zitierten Internetquellen wurden zuletzt am TT.MM.JJJJ aufgerufen.

RFID and Evidence Based Stock Management

Catherine Cooke

I should like to thank the Technische Hochschule for giving me the opportunity to talk about what we've been doing with Stock Management and RFID hand-held scanners. Much of this presentation is inevitably about the systems we use in Westminster – Sirsi-Dynix Symphony and Intellident RFID scanners – other products are different.

I should perhaps explain a little about Westminster Libraries. We are the public library service for the City of Westminster, one of the 33 London boroughs and one right at the heart of London. We have 11 libraries, 2 satellite Libraries, an Archives and Local History Centre and a Home Library Service. We have nearly 3 million visits a year and a membership of around 87,000 with a 30 % annual turnover. As a central London authority we have a relatively small resident population, but a very large daytime population. We hold some 1 million items in stock, with about 2.5 million items loaned annually. There are 195 staff (140 full time equivalent posts). We have some of the longest opening hours in London. Our earliest opening is 7.30am at Pimlico Library, a new library which shares its building with a school and Adult Education Centre, offering services to them as well as serving as the local library for Pimlico. Our latest closing is 10pm at Paddington Library. 5 of our libraries are open on Sundays.

While we do have long-standing members, much of the population is transient – they come and live in Westminster for a year or two, then move on. Our membership and visitor figures have been generally rising over the last 5 years and this at a time when national trend has been that they are dropping. We run customer satisfaction surveys every couple of years and the results show the service as good and improving – 90 % of our users say the service is Good or Very Good.

Westminster Libraries are very busy and active with relatively few staff, especially in the traditional »back office« areas such as Acquisitions.

We have been using RFID for some 4 years now, implementing Intellident equipment from 2007 first in our 4 largest libraries. As a general rule we have 3 self service machines in each library offering issue, renewal, discharge and payment, as yet taking coins only. We regarded it as a transformation of the service because as self-service went in we, as others have already mentioned they did, removed the big old counters and installed smaller staff desks away from entrance. When you enter the library the first thing you see is the self-service – the counter is further back. Staff are no longer behind counters but out in the library floor-walking in a similar way to shop staff. They take customers to self-service and train them. Our non-book material, DVDs and CDs, are open access.

Westminster is a relatively small geographical area – you can travel by public transport from a library at one end to one at the other in about half an hour. Many customers use more than one library. We therefore tagged all lending stock at the beginning of the implementation, the work being done by temporary staff working in teams round the libraries. All staff stations were equipped with RFID pads and software. Over the next couple of years, as libraries were refurbished or, in the case of Pimlico, relocated, we took the opportunity to introduce self-service. All libraries are now fully self-service.

With the introduction of RFID, stock items no longer have a date label to indicate their last issue date or how often they are used. Both the self-service kiosks and any staff issues give the customer a receipt with the due date on it – plus it acts as a bookmark!

I am including a few examples of scanners available in England – this is one from Bibliotheca.

So how does one approach Stock Management in this day and age? The traditional way when I started years ago was to look at the date labels. We stopped using date labels when we moved to RFID for self-service and staff issue – we give a receipt instead

You could run reports off the LMS. Standard reports are available on Symphony which could extract the data, or you could use an external Reporting Tool such as Crystal Reports or Cognos Impromptu. Both these methods, however, require staff with a significant understanding of the database structure to set up and run reports and they are time consuming.

We use Evidence Based Stock Management software, a system called SmartSM from the company BridgeAll. There is an automated monthly data extract from Symphony to a separate database system. This is scheduled at 9.15am on the 1st of every month and takes just under half an hour. The extracted file is automatically sent by ftp to BridgeAll, where it is automatically loaded into SmartSM and made available. The result is presented in a web interface with pre-designed tailored reports. We made decisions centrally about the parameters used in these reports and they can be changed for specific reasons, or for specific sites where different parameters would better suit the library. The system is easy for staff to use with minimal training and there is no impact on the live Symphony system.

Lists of stock can be printed off and staff search manually for the items – that is how we started. Now there is also an option to download the reports to a hand-held scanner – such as to this example from 3M. Again there is a parameter to specify which company's scanner is in use in the authority.

We've concentrated on two areas of SmartSM using Stock Management software – there are other facilities within it.

Dead Lists

Dead Lists – items that have not been issued for a significant period of time. It is up to the library to decide what they regard as significant. A fiction book not issued in over 6 months might be considered 'Dead' and should be removed. For non-fiction, you might give it 1 year. We are a public library. One of our main success indicators is the number of issues. If an item is not earning its place on the shelves, it should be removed and replaced with a newer, better, more attractive item that will earn its place. I should add that we do keep material for more than this, classics such as Dickens' work for instance. Check the shelves, delete those items you find you don't want to keep, ISSUE and DISCHARGE those you want to keep so they don't come up as unused again for a while and finally delete everything you can't find.

Grubby Lists

Grubby Lists – items that have been issued a certain number of times. A book that has been issued 25 times might be considered 'Grubby' and should be removed. If it's a children's book, you might think 15 or 20 times would be enough to wear it out. These items are popular and still being used – maybe one grubby hardback should be replaced with 2 bright new paperback editions. This is an alert to items to consider, it is not a categorical instruction to delete something. You might decide to keep it because there are no paperback versions of that title on the shelves, it is still in good condition or it is out of print and impossible to replace. Check shelves for books, delete those you find you don't want to keep, consider reserve stock for those you feel worth keeping but that aren't really in good enough condition for the open shelves, and again, delete everything you can't find. This is the scanner from D-tech.

This is the Intellident scanner we are now using. RFID is often seen as self-service, but it is potentially much more.

The delivery of original hand-held scanners was in mid-Oct 2008. They were a different, bigger design and there were a few teething problems, particularly around the battery life of hardware. You could scan for about 2 hours, then you had to recharge them overnight before you could do anything else. New equipment was released which we purchased about 18 months ago – this one. It's a Nordic scanner with a multi-directional antenna designed in UK by Intellident. You can use it in this orientation if you are scanning books shelved normally, or twist it through 90 degrees and down to scan racks of DVDs or CDs. This means you can easily keep the antenna in the same orientation as the tags, but still hold the scanner comfortably and see the screen. The battery life is much

better – 6 to 8 hours – and you can upload and download reports while recharging. It sits in a cradle connected to the PC by USB when not in use. This is the one we are using now.

As these are stock functions, they are largely bound up with Symphony which has three processes for RFID stock work:

Shelf tidy

Shelf tidy – This is not an immediate priority for us. We are a public library and do not use long Dewey classification numbers. Stock is shelved in broad subjects like Science or Photography and staff can tidy shelves by eye quite easily.

Search

For this you run a program on Symphony or download a file from SmartSM, then download the result to the hand-held unit via a PC. You scan the shelves, recharging as necessary. The scanner bleeps to alert you when it finds an item and displays brief details on the screen so you can take it off and deal with it there and then or put it to one side to deal with later. You then upload the result to Symphony and run another program to update the catalogue. If you search for items with a particular status, perhaps with reservations or a status like In Processing, those not found are marked MISSING by the report processing the result file.

Inventory

For this you take a blank hand-held scanner and scan shelves to capture the items. You upload the resulting file to Symphony and run a program to process it. For every item found on the shelves, the program enters the date you run this program in an Inventoried field on the records of items. Items not scanned on the shelves are left with NEVER or an old date in the Inventoried date.

The first case study was done with the old scanner. I searched Marylebone Library Adult stock for over 1,000 MISSING items, a process which took 5 hours. We mark anything we cannot find as MISSING, usually as the result of looking for it for a reservation. Marking it MISSING allows the LMS to try the next library that should have a copy, and prevents time being wasted looking for the same thing in the future. Staff do not, however, have time to go and look again several weeks later for these items, so unless someone happens to borrow them, they tend to stay marked MISSING.

In a second pass I inventoried all Marylebone Adult Fiction in about 3 1/2 hours, which gives an average of 1,500 items per hour – something absolutely impossible by traditional methods.

Books shelved normally and standing face on read well. Those lying flat on metal shelves do not – the tag is too close to metal. You just pick the book up and pass the scanner underneath it – it takes less than a second.

The scanner has a broad field – reading in advance of the antenna and above and below as well, so as you scan one shelf and back along the next, the scanner has a couple of opportunities to read tags. I also did some tests with programmed tags stuck on cards scattered on a desk, even partly piled up. The new scanner showed 100 % read rate with the scanner passed over them at a moderate speed. It is not so good if you go too fast.

Using a program on Symphony to create a search file takes time, maybe up to an hour to define and run it, being clear about matters such as which Library, Item Type, Item Category, Status/s to include/exclude and which date parameters you want. Data transfer between the scanner and the PC and between the PC and Symphony is very simple and fast, a matter of seconds only.

Processing the results of a search or inventory does take time though, about an hour for every 2,000 items. After an inventory, Symphony reports the barcode, shelf mark and brief author and title details, plus the date of issue for items reported on loan, so you investigate those *before* the date of the scan, which is useful when you are building up a scan over several days. You can then do a manual search for various items reported on loan, in transit, at a library other than the library scanned or those that did not match in the catalogue (the report gives the identity of an item scanned near the one that could not be matched).

Deleted items do seem to find their way back on to the shelves from time to time. I suspect a lot of what was on the shelves that shouldn't have been was down to customers not putting items where the self-service kiosks tell them to, especially in the early days of self-service. We do not have sortation units – we do not have the space in our libraries and our throughput is not high enough to justify them. Our kiosks do a basic sort. If an item requires attention – transit to another library, is reserved or a DVD or CD whose case needs relocking – the kiosk displays a big red arrow pointing to a closed box. If an item should just be shelved, it displays a big green arrow pointing in the other direction to a trolley. I have watched someone when the kiosk displayed a red arrow put the item on the trolley the other side, and when it displayed the green arrow, put the item in the closed box! We do not check the items on trolley. If someone else has not already borrowed something by the time we deal with the items on the trolley, we just reshelve them.

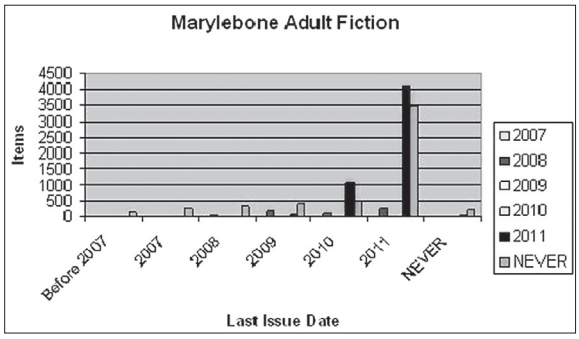
Case study 2 was done using a Grubby Stock list from SmartSM. I pulled off Marylebone Grubby »Hardback Fiction« to my PC, connected the handheld and transferred the file, a process which took about 5 minutes. This is to be compared with about an hour using Symphony to crate the file and had no effect on the System – it doesn't risk slowing it and you don't have to avoid other reports that run at specific times.

It took me 1 hour 40 minutes to search Marylebone's Adult Fiction for 248 items. I found 150. Of the remaining 72, 64 were on loan, 1 on the hold shelf and 7 marked Missing. This is a rate of 1 ½ items a minute – absolutely impossible searching by eye. Indeed it was so fast that I had to take the scanner away from the shelves from time to time as I couldn't pull the books off as fast as it was finding them. In fact, the Library Manager was

quite interested and pulled a book off the shelves a few feet in front of me that she felt was grubby. We held it to the scanner and it bleeped – it was one of the books it wanted.

I uploaded the results file to Symphony, the first time I had started from SmartSM and uploaded back to Symphony. It reported the right numbers and listed all the items on loan or Missing. It inventoried found items as expected. As it was a very small file, it didn't take long to run.

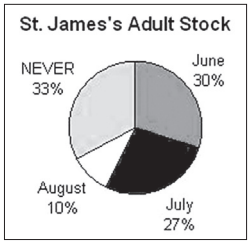
Pulling a file like this from SmartSM is *vastly* quicker and easier than creating the report on Symphony. It opens the process to anyone we can give access to SmartSM without any impact on the system. We do not let just anyone have access to Symphony reporting – only a few trained staff. Searching by eye for items on a report like this is not easy and very frustrating as 44% of items included shouldn't be on the shelves in the first place being legitimately on loan. I do feel is worth checking for items marked Missing or on loan – I found quite a lot of both on the shelves.



The coloured bars are the year when items were inventoried, set against a range of Last Issue Dates. Looking at the results in this graphical form, we can see there is a small amount of material that has not been issued for some years and NEVER inventoried. This may be accounted for by the fact that Symphony retains details if items with fines owing on them, even though the item itself has been physically withdrawn.

The third case study is a very recent one and I am still analysing the results. It was our first properly conducted inventory using a scanner. I should say that we have not run a proper catalogue clean-up for about 4 years.

There are three elements to an inventory:
- Run a program to mark all items currently out on loan as inventoried with the run date as the inventory date. This is the start date, in this case 1st June 2011.
- Run a program early every morning to mark as inventoried all items issued the day before.
- Scan the stock on the shelves.

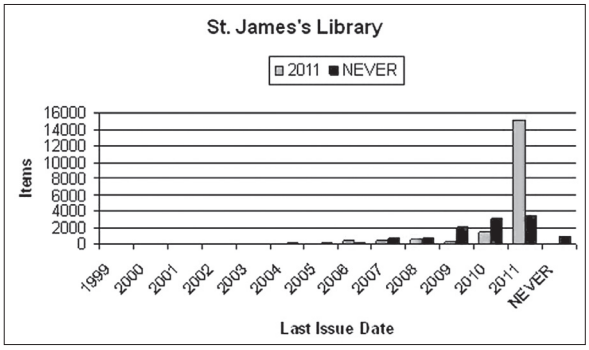


This means you only have the one field to worry about – the Inventoried field. At the end of the three months, anything that has either NEVER or a date *before* the start date in the Inventoried Date probably no longer exists and can be removed from the catalogue.

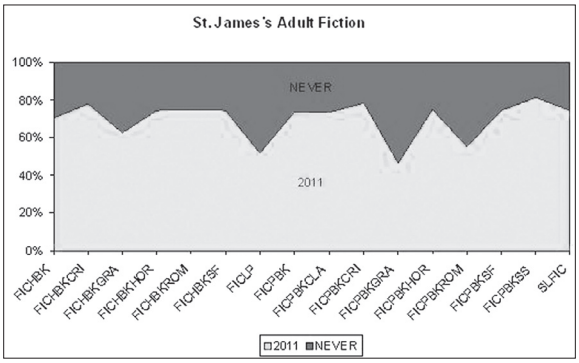
The pie chart shows the percentage of stock inventoried each month. I have to admit that 33% NEVER inventoried seems

rather high. It may be that staff did not complete the Adult stock in the limited time available for this project and stock already marked MISSING may be included. On the other hand, another London authority did a similar exercise in their Central Library recently using another company's scanners – they found 25 % of the stock did not get inventoried. Again this is probably higher than you'd expect. It raises questions about what happens to stock, questions probably better investigated in due course once an initial complete inventory has been done for the first time in many years. There's too much unknown over too long a period at present.

Last Issue	Inventoried 2011	Inventoried NEVER
1999	0	48
2000	0	14
2001	0	50
2002	0	48
2003	1	51
2004	1	144
2005	27	106
2006	398	139
2007	477	759
2008	563	752
2009	304	2016
2010	1467	3076
2011	15130	3395
NEVER	39	920



This is looking at this stock broken down by Date of Last Issue. If something has not been out for years and was not picked up in the Inventory, it probably does not exist. For instance, 27 items last issued in 2005 were inventoried on the shelves; 106 were not – the 106 probably no longer exist. In fact we'd probably also wonder if the 27 are worth keeping since no one seems to want to borrow them!



You can also drill down to specific stock areas to see the proportion of stock NEVER inventoried in particular areas. This shows our various Fiction categories – paperback, hardback, crime, romance etc. St. James's Library is a small library, so there are only a few items in some of the categories, so the percentages can be a bit misleading. This merely shows that once you have the data collected and uploaded to the catalogue, you can look at it in different ways.

We have 7 hand-helds and 11 libraries, so we will probably base them at the larger libraries and they share them with the smaller ones. We also need to install the relevant Intellident software on PCs, creating the necessary file structures. We in Libraries are not allowed to do this and must wait for our Corporate IT support people to do it for us. We also need to add the Symphony utilities and reports to specific user profiles so they can upload data from the scanners to update the catalogue. Staff generally do not

have the permission to run reports on Symphony. There are constraints on staff time and administrative considerations on Symphony, so there will be a support overhead for using the scanners. Uploading and running the programs does have to be managed, so staff will save the files and send them as an attachment to a named person, probably in the Stock Team. They can then schedule and run the programs, making sure they do not interfere with other programs that are already scheduled. Holding files on the PC have a limit of one file at a time and on Symphony you can have only one file per library. 1 file on scanner can have multiple sub-files.

These are the sorts of tasks we have in mind for the scanners:
- Frequent periodic checks for items marked MISSING or reserved items
- Annual Inventory of library, maybe rolling basis
- Search for items lost in transit
- Search for items reported lost
- Search for items added by EDI Order Fulfillment not in available stock

You do not actually have to upload the results every time, but it does help keep the catalogue clean and pick up anomalies. A Good Thing – BUT it takes time. Keeping the catalogue clean means customers and staff do not waste time looking for items the catalogue says we have but which in fact cannot be found. As some services are charged by catalogue size, having dead wood in there may be costing you money better spent elsewhere.

I did get a lot of comments about the hand-held scanners from staff »When are we getting one?« and from customers – one asked me »Are you disinfecting the books?« Staff were keen to get their hands on them and I got the feeling they'd rather search for missing or lost items with a scanner than with a huge sheaf of paper print outs.

How long does it take to search 5 or 6 thousand books subdivided into sections by genre for 248 items by eye with a sheaf of paper? It's a long time since I've done that, but I suspect a *lot* longer than 1 hour 40 minutes.
- Catherine Cooke ccooke@westminster.gov.uk
- Intellident Ltd. http://www.bibliotheca.com
- SirsiDynix http://www.sirsidynix.com/products/symphony
- SmartSM http://www.smartsm.com/

This is my e-mail address in case anyone wants to follow any of this up and contact details for the UK arms of the companies we work with – I don't know their penetration in mainland Europe. Intellident as we have heard, merged with Bibliotheca earlier this year.

Inventur mit RFID-Handlesegeräten
Erfahrungsberichte über die Durchführung von Inventurarbeiten mit Hilfe von RFID-Handlesegeräten

Jan Kissig, Doris Köhler

Dieses Kapitel behandelt das Thema der RFID-gestützen Revisionsarbeiten in Bibliotheken anhand zweier Beispiele und zeigt auch selbstentwickelte Ansätze auf, die die Durchführung der Arbeiten effizienter gestalten. Im Grundlagenteil werden die verschiedenen Voraussetzungen für Inventuren mit RFID beschrieben: der Listenim- und export aus dem Bibliotheksmanagementsystem, das Handling der Handlesesgeräte sowie der Transponderposition im Buch. Am Beispiel der Bibliothek der TH Wildau werden ältere Ergebnisse von Testinventuren aus 2008 mit aktuellen Tests aus 2011 verglichen. Eine eigene Inventur-Software und die Nutzung der transponderspezifischen Seriennummer als Mediennummernersatz werden hierbei eine Rolle spielen. Am Beispiel der Universitätsbibliothek Bielefeld wird die Entwicklung eines Revisionstools, in Kooperation mit der Firma Bibliotheca RFID, sowie deren Testergebnisse und der Echtbetrieb beschrieben.

Einleitung

Inventuren sind für Bibliotheken ein wichtiges Instrument der Bestandskontrolle. Nicht nur verloren gegangene Medien werden ermittelt, auch die Wiederherstellung der Ordnung in den Regalen sowie die Aussonderung alter Bestände kann dabei erfolgen. Doch die Durchführung einer Bestandsaufnahme ohne RFID ist oftmals mit großem Aufwand (Personalbindung und eventuelle Schließzeiten) verbunden, da die Medien jeweils optisch erfasst, und mit einer Sollliste abgeglichen werden müssen.

Der Einsatz von RFID kann diese Schwierigkeit umgehen, da fast zeitgleich mehrere Medien von einem Lesegerät erfasst und auf Validität überprüft werden können[1]. Damit eine Inventur mit RFID auch reibungslos funktioniert, bedarf es jedoch einiger Voraussetzungen, welche im ersten Abschnitt dieses Kapitels benannt werden.

Bis eventuell in Zukunft die Buchregale intelligent sind, also sog. Smart-Shelves genutzt werden (Regale die per RFID selbständig ihren Bestand auswerten), müssen Inventuren weiterhin mit Handlesegeräten durchgeführt werden. Eine weltweite Umfrage zu Handlesegeräten zeigt zwar mittlerweile eine höhere Performance und Zuverlässigkeit solcher Geräte, jedoch sind die Eigenschaften für mehr als 30 Prozent der Anwender noch immer nicht ausreichend [2].

1 Z. B. 20 Medien/s Bibliotheca Smartstock 100/110 [1]; Eigene Tests ergaben bis zu 50 Medien/s (siehe Abschnitt Inventur über UID)

Inventuren sind dennoch ein spannendes Anwendungsfeld für den Einsatz von RFID. Aus dem Beispiel der Handelswirtschaft folgend, wird auch durch die Verbreitung von RFID in Bibliotheken, der Einsatz dieser Technik für Revisionsgänge noch immer als Kernanwendung gesehen.

Inventur mit RFID an der TH Wildau [FH]

In diesem Abschnitt sollen die verschiedenen Voraussetzungen und Arbeitsschritte für eine Inventur am Bestand aufgezeigt werden. Durchgeführt wurden die auf den Text aufbauenden Tests an der Bibliothek der Technischen Hochschule Wildau im Jahr 2008.

Voraussetzungen

Die erfolgreiche Durchführung einer Inventur bedarf vieler verschiedener Arbeitsgänge. Das Grundprinzip einer Inventur mit RFID besteht aus dem Abgleich, einer vom Bibliothekssystem generierten Bestandsliste und einer vom RFID-Handlesegerät generierten Liste. Wie diese Listen erstellt und abgeglichen werden können, wird in den nächsten Abschnitten beschrieben.

Listenerstellung über das Library Management System (LMS)

Das Library Management System (LMS) bildet die Grundlage für die Durchführung von Inventurarbeiten, da aus diesem System heraus der aktuelle Bestand hervorgeht.

Zum aktuellen Bestand werden alle nicht entliehenen Medien in einer Liste zusammengefasst. Grundbestandteil dieser Liste ist die eindeutige Referenz zum Medium welche auch auf dem Transponder im Medium gespeichert ist, im Normalfall die Mediennummer. Der Übersicht halber sollten auch andere medienspezifische Daten, wie Signatur und Titel, Bestandteil dieser Liste sein. Das von uns in der Hochschulbibliothek Wildau verwendete Inventurgerät konnte für verschiedene Listenformen konfiguriert werden, wobei eine Form bestehend aus Mediennummer und Signatur ausreichend ist um das Buch per Funk und visuell abgleichen zu können. Das RFID-Lesegerät stellt einem dazu die Buchdaten auf dem Display zur Verfügung[2].

```
„Mediennummer" | „Signatur" | „Titel"

200900123 | 0TRX1 | Java Codebook
200800456 | 0TRX2 | PHP und MySQL
```

Abb. 1: Struktur der Medienliste für das RFID-Handlesegerät.

Für die Listenerstellung benötigt das LMS eine Exportschnittstelle, die im Fall von z. B. Sisis Sunrise V3.6 nicht zur Verfügung stand. Eine Bestandsliste muss somit per Datenbankabfrage manuell erstellt werden. Durch die manuelle Erstellung kann die Liste

2 Es werden nur Buchdaten dargestellt, die in einer Bestandsliste enthalten sind. Diese muss zuvor auf dem Gerät importiert werden.

allerdings auch genau an eigene Bedürfnisse angepasst werden. Beispielsweise können nur Medientypen in die Liste aufgenommen werden, welche sich auch wirklich im entsprechenden Regal befinden sollen (Monographien, Lesesaal, DVDs). Audiokassetten und andere Medientypen, welche gesondert aufgestellt sind, müssen somit nicht erfasst werden.

SQL-Beispiel:

```
select Mediennummer,Signatur
from Buchtabelle
where Ausleihstatus = 'nicht entliehen'
and ( Medientyp = 'Lesesaal' or Medientyp = 'Monographie' or
Medientyp = 'DVD' )
and ( Signatur like '[01][ ]A%' or Signatur like '[01]A%' )
order by Signatur
```

Abb. 2: Beispiel für eine Datenbankabfrage

Vorteilhaft für eine solche Liste ist, wenn diese auch der Medienreihenfolge im Regal entspricht, um eventuelle Probleme auch leichter anhand von gescanntem Vorgänger oder Nachfolger nachvollziehen zu können. Für den Fall, dass die Liste nicht sortiert vom LMS erzeugt wird, ist es möglich die reinen Textdaten anderweitig (z. B. mit einem Officeprogramm) nach der Signatur sortieren zu lassen.

Die Bestandslisten (Solllisten) können nun auf das RFID-Handlesegerät importiert werden.[3] Das Handlesegerät erfordert allerdings nicht zwingend den Import einer solchen Liste, da es selbst eine erstellt, die wiederum über eine geeignete Middleware mit der Sollliste des Bestands verglichen werden kann.

Nach dem Inventurdurchgang bedarf es dann einer weiteren Möglichkeit, die Ergebnisse in das Bibliothekssystem einzuspielen um nicht gefundene Medien zum Beispiel als Verlust zu buchen. Auch hier bietet sich keine geeignete Schnittstelle an, so dass alle Medien manuell in den LMS-Clients nachbearbeitet werden müssen.

RFID-Handlesegeräte

Für unsere ersten Inventurversuche im Jahr 2008 standen uns zwei verschiedene Bauweisen von RFID-Handlesegeräten der Firma Bibliotheca RFID Library Systems zur Verfügung (BiblioWand und BiblioWand Light). Beide Geräte waren sehr handlich und mit einem PDA für die Visualisierung der Ergebnisse ausgestattet. Einzig die Antennen unterschieden sich im Design, so dass eine Antenne mit einem externen Akku über ein Kabel versorgt wurde, während die andere über einen internen Akku verfügte. Die Datenübertragung zum PDA wurde bei einem der Geräte über ein Kabel, beim anderen über Funk (Bluetooth) realisiert. Dies bietet den Vorteil, dass man den PDA in das Regal legen kann um mit der nun freien Hand Bücher für eine bessere Lesbarkeit der Transponder aus dem Regal zu ziehen.

3 Funktionierte nur mit Bereichslisten (wenige Tausend Medien)

Der Unterschied zwischen den Antennenbauformen äußerte sich nur durch eine geringfügig bessere Transpondererfassung bei dem Gerät mit der Schwertantenne. Dieser Vorteil wird aber durch die leichtere Handhabbarkeit des kabellosen Gerätes ausgeglichen.

Abb. 3: Bei uns eingesetzte RFID-Handlesegeräte (bibliotheca-rfid.com)

Beide PDA-Einheiten verfügen über WLAN-Funktionalität, welche es theoretisch ermöglichen würde direkt mit dem Bibliothekssystem zu kommunizieren. Beim Test stand allerdings keine solche Verbindungsmöglichkeit zur Verfügung.

Mit den auf das Gerät kopierten Solllisten kann dann der Scanvorgang am Regal beginnen. Die Liste kann ebenfalls als Suchliste genutzt werden. Somit wird bei einem Medium, dessen Mediennummer sich nicht in der Liste befindet, ein Alarm ausgelöst und das Gerät zeigt einem die Mediennummer an.

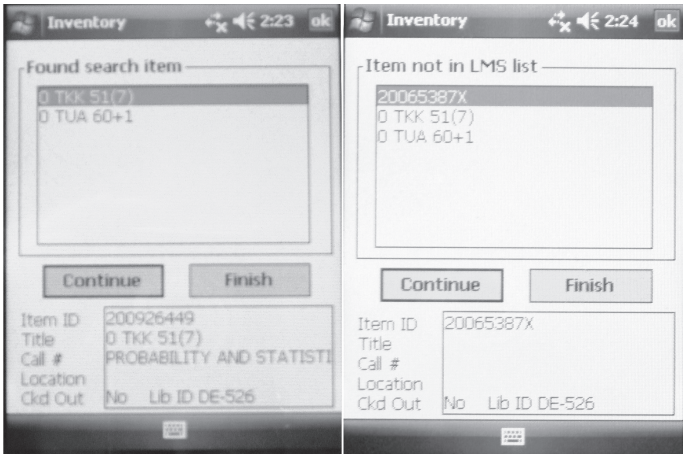


Abb. 4: Benutzeroberfläche BiblioWand (Quelle: Kissig)

Bei einem Inventurdurchgang mit Sollliste und gleichzeitigem Nutzen der Suchfunktion auf dem Gerät, wird dann automatisch eine Liste von Verlusten (nicht gelesen), eine Liste der abgearbeiteten Suchliste und eine Liste mit allen gefundenen Mediennummern erstellt. Allerdings bestehen diese nur aus der Aneinanderreihung der Mediennummern, es wird einem keine Signatur zur einfachen Nachbearbeitung angeboten.

Positionierung der Transponder

Die richtige Position der Transponder in einem Buch spielt eine wichtige Rolle für eine hohe Erkennungsrate durch die RFID-Handlesegeräte, da diese bedingt durch ihre Bauform nicht immer den optimalen physikalischen Eigenschaften eines RFID-Systems entsprechen. Gemeint sein können hier zum Beispiel die senkrechte Ausrichtung der Antenne zum Transponder oder auch der Versatz des Magnetfeldes bei einer parallel geführten Antenne.

Abb. 5: Auslesen der Transponder mit dem Handlesegerät (Quelle: Seeliger)

Die durch die Bauform und Größe der Transponder bedingte Positionierung im Innenteil des Buches, nicht auf dem Buchrücken, fordert daher einen Bereich zum Kleben nahe am Buchrücken. Dies ermöglicht, durch einen geringen Abstand zur Lesegerätantenne, eine erhöhte Erkennungsrate der Transponder. [3]

Des Weiteren sollte bei einer Benutzung von Metallregalen auch ein Mindestabstand der Transponder vom Regalboden eingehalten werden. Dieser verhindert eine Dämpfung des Magnetfeldes durch induzierte Wirbelströme im Metall und erhöht somit die Erkennungsrate der Transponder. [4]

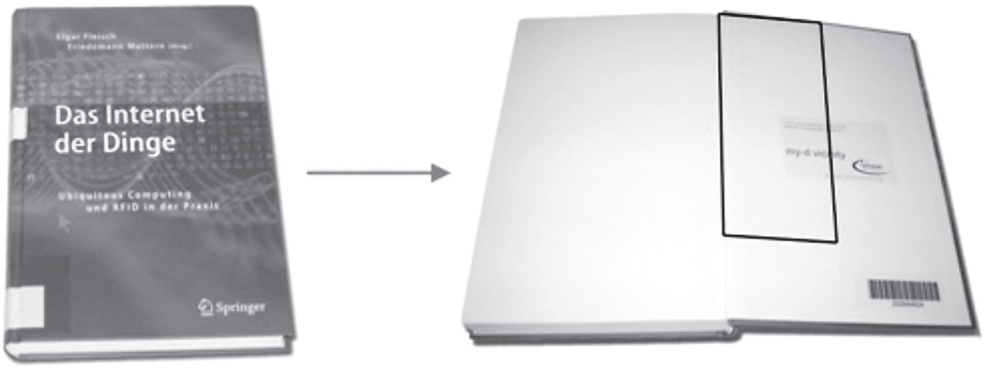


Abb. 6: Positionierung der Transponder (Montage: Kissig)

Für Zeitschriften und andere dünne Medien bietet es sich an, in der Klebehöhe zu variieren, damit die Transponder von außen gesehen nicht direkt aufeinander liegen. Ein Aufeinanderliegen führt zur gegenseitigen Verstimmung der Transponder und mindert die Erkennungsrate deutlich. [3] Bei modernen Transpondern scheint dieses Problem allerdings behoben. So ergaben Tests vor Ort, bei 10 übereinanderliegenden Transpondern mit I-CODE SLIX-Chip, eine erfolgreiche Erkennung durch das Lesegerät.

Abb. 7: Transponderpositionierung bei dünnen Medien (Montage: Kissig)

Middleware

Eine Middleware ist für die Durchführung einer Inventur ein wichtiges Werkzeug. Dieses Programm kann zum Beispiel für die Erstellung von Bestandslisten und den Vergleich der Ergebnislisten genutzt werden. Zusätzliche Funktionen, wie Listen von stark oder nicht frequentierten Medien können als Suchlisten dienen. Weitere Beispiele für die Funktionalität einer Middleware sind im Abschnitt »Einführung eines Revisionstools an der UB Bielefeld« aufgezeigt.

Eine beim Revisionstest 2008 an der TH Wildau eingesetzte Software (Eigenentwicklung) kann einen Abgleich von 2 Listen (Soll und Ist) durchführen und erstellt daraus zwei

neue Listen bestehend aus Versteller- und Verlustexemplaren. Die Anwendung bietet durch Anbindung an die LMS-Datenbank auch die Funktion, Daten wie Signatur und Titel den Mediennummern zuzuordnen.

Die eingesetzten RFID-Handlesegeräte unterstützten diese Listenerstellung ebenfalls, allerdings fehlte zur Nachbearbeitung (Ermitteln der Signatur), eine Anbindung an das Bibliothekssystem.

Der Einsatz von Middleware ist, wenn sie nicht in der Software vom RFID-Inventurgerät untergebracht ist, von großem Vorteil, da diese direkt mit dem LMS kommunizieren kann, um zum Beispiel nicht gefundene Medien automatisch als Verlust zu buchen.

Testszenarien unserer Teilinventur (2008)

In diesem Abschnitt werden verschiedene Testszenarien, welche bei uns durchgeführt wurden genauer erläutert. Die Testszenarien beschreiben die Medienaufstellung in den Regalen. Dies ist wichtig, da genau diese Aufstellung zu einem gelungenen Inventurdurchgang führen, oder diesen erheblich behindern kann.

Testszenario 1 – Nachschlagewerke

Beim ersten Testszenario handelt es sich um Regale mit Nachschlagewerken. Diese sind, aufgrund ihrer Buchrückenbreite besonders gut zum Auslesen mit dem RFID-Handlesegerät geeignet, da die Transponder räumlich meist weit auseinander liegen.

Testszenario 2 – Lehrbuchsammlung

Beim zweiten Testszenarion handelt es sich um den Bereich der Lehrbuchsammlung. Hier befinden sich, ähnlich wie bei den Nachschlagewerken, immer ähnliche Medien im Regal. Dabei kommt es hierbei aber öfter zu Medien mit einem dünnen Buchrücken, und aufgrund ihrer großen Anzahl, kann das somit ein Problem für das RFID-Handlesegerät darstellen.

Testszenario 3 – Freihand

Beim dritten Szenario handelt es sich um die Freihandaufstellung. Hierbei stehen Medien unterschiedlicher Buchrückenbreite in einem Regal.

Mit 25 bis 35 Medien pro Regalmeter haben wir im Vergleich zur durchschnittlichen Belegung mit 20 bis 30 Medien eine teilweils hohe Mediendichte [5].

Das Szenario der Freihandaufstellung entspricht allerdings am ehesten dem Bestand einer wissenschaftlichen Bibliothek und damit bedürfen die Inventurarbeiten hier der größten Anstrengung gegenüber den vorherigen Szenarien.

Durchführung

Vor der Durchführung von Inventurarbeiten sollte man stets darauf achten, dass die Geräte vollständig geladen sind.

Des Weiteren sollte man die Bestandslisten für die RFID-Handlesegeräte zeitnah erzeugen, so dass man sichergehen kann, dass in der Zwischenzeit keine Medien aus dem Regal entnommen wurden.

Ausgestattet mit dem Handlesegerät und der aktuellen Bestandsliste geht man nun Reihe für Reihe die Regale ab. Die Antenne des Lesegerätes muss dafür sehr nah am Buchrücken in Höhe der Transponderposition entlang geführt werden. Als Richtgeschwindigkeit dient laut Gerätehersteller ein Wert von ca. 1 Meter in 10 Sekunden. Während des Scannens sollte man stets den Blick auf den PDA-Bildschirm richten um abschätzen zu können, ob das Gerät auch möglichst alle Medien erfasst. Dies ist besonders wichtig bei vielen aufeinander folgenden Medien mit dünnem Buchrücken, da die Transponder für das Lesegerät sehr schwer zu lesen sind. Falls ein kabelloses Handlesegerät benutzt wird, kann man den PDA in einem solchen Falle in das Regal legen und mit seiner freien Hand die dünnen Medien einzeln leicht aus dem Regal ziehen, so dass eventuell übereinander liegende Transponder wieder getrennt werden.

Je nach Gerätekonfiguration wird einem bei Verwendung einer Suchliste vom Gerät eine Rückmeldung gegeben, falls ein Medium gelesen wird, welches sich nicht in dieser Liste befindet. In diesem Fall ertönt ein Warnton und die Mediennummer des Verstellers wird auf dem Bildschirm angezeigt. Diesen Versteller unter all den anderen Medien herauszufinden kann sich allerdings als schwierig herausstellen, da das Handlesegerät nicht die Signatur des Mediums ermitteln kann. Theoretisch sollte diese Funktion allerdings verfügbar sein, nur das verwendete Gerät konnte eine Liste unseres Gesamtbestandes mit knapp 90.000 Titeldaten (Signatur, Mediennummer und Titel) nicht laden. In diesem Fall hilft dann nur die Suche nach einer möglichen falschen Signatur oder die Nutzung des LMS zur Ermittlung des verstellten Mediums.

Nach dem abgeschlossenen Lesedurchgang erstellt das RFID-Handlesegerät folgende Listen:
- Liste aller Mediennummern, die vom Gerät gelesen wurden,
- Liste von Medien, die aus der Suchliste gefunden wurden[4*],
- Liste von Medien, die aus der Suchliste nicht vom Gerät gefunden wurden[4*].

Bestandteil all dieser möglichen Ergebnislisten sind allerdings nur die Mediennummern und da sich diese nur auf den Innenseiten der Bücher befinden, ist eine einfache Suche nach nicht gelesenen Exemplaren nicht möglich. Hier kam uns dann der Einsatz unserer Middleware zugute. Die Listen wurden vom Gerät exportiert und mit der Middleware eingelesen. Per Datenbankabfrage wurden die einzelnen Mediennummern mit den dazugehörigen Signaturen erweitert.

4 *optional, je nach verwendeter Gerätekonfiguration

Als nächster Arbeitsschritt folgte nun das Aufsuchen der Medien, welche laut RFID-Handlesegerät nicht gefunden wurden (Nachkontrolle). Hierbei haben wir dann eine auf Papier gedruckte Liste genutzt um die Signaturen optisch abgleichen zu können. Es wäre hierbei auch möglich gewesen eine Liste für das RFID-Gerät zu nutzen, jedoch fehlte dem Gerät die Möglichkeit, einem die gesuchten Signaturen im Display anzuzeigen. Diesen gesamten Arbeitsschritt haben wir bei der Ergebnisbetrachtung dann als Aufwand für die Nachbearbeitung angegeben. Medien, die bei dieser Suche nicht im Regal gefunden werden, müssen dann im Bibliothekssystem von Hand als Verlust gebucht werden. Auch hier fehlte die Möglichkeit, dies zu automatisieren.

Ergebnisse

Die Ergebnisse erhalten wir durch mehrfache Lesedurchgänge für die verschiedenen oben genannten Testszenarien. Die Werte in den Tabellen sind gemittelte Werte. Für die Szenarien Nachschlagewerke und Lehrbuchsammlung haben wir uns auf nur einen Bereich beschränkt, das Szenario Freihandaufstellung haben wir an mehreren Bereichen durchgeführt, da diese einer durchschnittlichen Aufstellung am ehesten entsprechen und gesondert betrachtet werden müssen.

Verlustexemplare sind aus den Solllisten bereits herrausgerechnet. Das Auffinden nicht gelesener Medien ist in der Dauer für die Nacharbeit enthalten. Die Nacharbeit umfasst das Nachschlagen von Signaturen und das Suchen dieser im Regal.

Ergebnis Testszenario 1 – Nachschlagewerke

#	Anzahl Medien laut LMS	Mit RFID erfasst	nicht erfasst	Dauer Scannen	Dauer Nach-Arbeit	Detektions-rate (%)
1	741	721	20	8	20	97,3

Tab. 1: Detektionsrate vom RFID-Handlesegerät bei Nachschlagewerken (gemittelt)

Im Bereich der Nachschlagewerke zeigen sich die Stärken einer mit RFID durchgeführten Inventur. Wir erreichten eine durchschnittliche Detektionsrate von 97,3 Prozent.

Ergebnis aus Testszenario 2 – Lehrbuchsammlung

#	Anzahl Medien laut LMS	Mit RFID erfasst	nicht erfasst	Dauer Scannen	Dauer Nacharbeit	Detektions-rate (%)
1	291	283	8	4	9	97,3

Tab. 2: Detektionsrate vom RFID-Handlesegerät bei Lehrbuchsammlungsaufstellung (gemittelt)

Ein ähnliches Ergebnis erhalten wir auch bei den Lesedurchgängen im Bereich der Lehrbuchsammlung.

Ergebnis aus Testszenario 3 – Freihand

#	Anzahl Medien laut LMS	Mit RFID erfasst	nicht erfasst	Dauer Scannen	Dauer Nacharbeit	Detektions-rate (%)
1	741	721	20	8	20	97,3
2	581	564	17	7	19	97,1
3	1500	1279	221	35	40	85,3

Tab. 3: Detektionsrate vom RFID-Handlesegerät bei Freihandaufstellung (gemittelt)

Hier zeigen sich bereits deutliche Unterschiede zu den vorangegangenen Messergebnissen. Die hier gezeigte Variation der Detektionsraten entstand durch den Umstand, dass bei einem der Bereiche eine hohe Anzahl an Medien mit dünnem Buchrücken vorlag.

Inventur über die UID (Unique Identifier) des Transponders

Grundlagen UID und Mediennummer

Die UID eines Transponders ist seine eindeutige Seriennummer, die bei der Produktion fest auf dem Speicher des Chips geschrieben wird und unveränderlich ist. Diese Nummer ist damit wie die Mediennummer einzigartig und kann für die Bestimmung des Mediums herhalten. [6]

Der Unterschied, der bei der ausschließlichen Nutzung der UID entsteht (UID und Mediennummer sind beide auf dem Speicher des Transponders hinterlegt) zeigt sich durch Geschwindigkeitsverbesserungen beim Auslesen und ist durch das Protokoll an der Luftschnittstelle bedingt[5].

Im Falle des Auslesens der UID wird nur ein einziges Kommando benötigt. Dieses Kommando (»inventory«) sorgt dafür, dass alle sich im Lesefeld befindenden Transponder mit ihrer UID zurückmelden. Der Inventorybefehl erfasst somit in einem Schritt mehrere Transponder.

Für das Auslesen der Mediennummer muss ein weiteres Kommando an den Transponder gesendet werden (»read multiple blocks«) wobei hier jeder Transponder einzeln angesprochen werden muss. Das bedeutet, dass bei X sich im Feld befindlichen Transpondern 1 mal der Inventorybefehl plus X mal der ReadMultipleBlocks-Befehl ausgeführt werden muss.

Ein weiterer Vorteil besteht durch die Länge der einzelnen Kennungen. Die Größe beträgt bei der UID 8Byte und bei der Mediennummer bis zu 16Byte (ISO28560-3 vormals Dänisches Datenmodell). [8] Je kürzer der zu lesende Datenblock ist, desto kürzer ist die Dauer für das Auslesen.

Voraussetzung hierfür ist jedoch die Speicherung der UID im LMS. Dies geschieht entweder in einem eigenen Feld, oder aber anstelle der Mediennummer, was einen großen

5 Beschrieben in ISO 15693-3[7]

Aufwand für die Änderung im LMS nach sich ziehen würde. Für die Konvertierung der Tags mit der UID, der Lösung mit dem zusätzlichen Feld, muss die UID mit der Mediennummer im LMS verknüpft werden. Des Weiteren muss eine Lösung für die Verknüpfung von Medienpaketen erarbeitet werden, da hier nicht wie üblich alle Transponder über die Mediennummer des Hauptwerkes als Paket zusammengefasst werden. Jedes Teil des Paketes verfügt mit der UID über eine einzigartige Kennung.

Performance

In eigens dafür durchgeführten Vergleichsmessungen wurden folgende Ergebnisse erzielt:

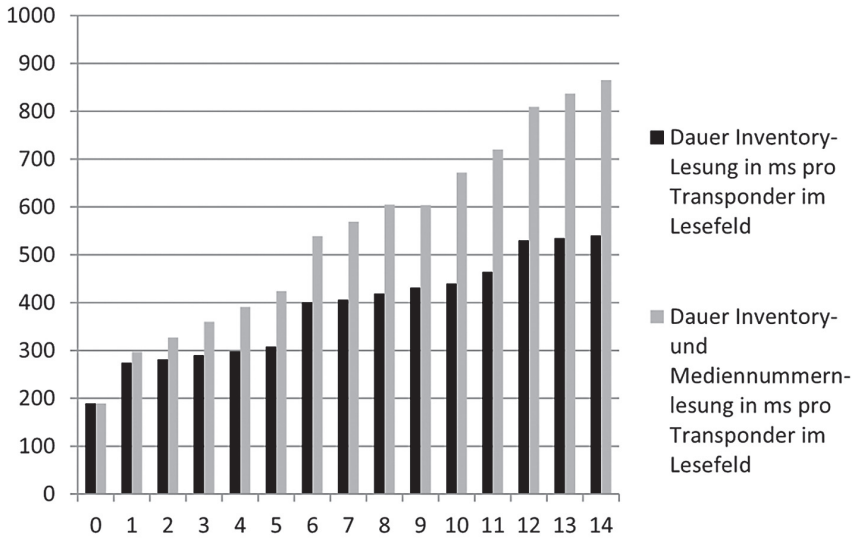


Abb. 8: Lesezeiten im Vergleich UID und UID+Mediennummer (Quelle: Kissig)

Beim Test wurden folgende Spezifikationen und Komponenten genutzt:
- RFID-Reader Feig ID ISC.MR101-U
- Antenne Feig ID ISC.ANTH200/200
- Feig Software Development Kit for Java
- Inventursoftware (Java, Eigenentwicklung)
- Länge der geprüften Mediennummer 9Bytes (3 Blöcke à 4Byte)

Es zeigt sich, dass sich das alleinige Auslesen der UID's der Transponder auf die Geschwindigkeit einer Inventur auswirken kann. Obwohl die Zeitdauer für das Lesen jeder einzelnen Mediennummer nur wenige Millisekunden beträgt (bei dieser Messung rund 23ms), was zum Beispiel bei 100.000 Medien theoretisch nur einen Mehraufwand von rund 40 Minuten bedeuten würde, bietet dieses Verfahren einen weiteren Vorteil: Die Gefahr, dass beim schnellen Abschreiten des Regals, Tags mit noch nicht gelesener Mediennummer sich schon wieder außerhalb der Reichweite der Antenne befinden, besteht nicht.

Test und Ergebnisse beim Verband der Öffentlichen Bibliotheken Berlins

Die im vorhergehenden Abschnitt aufgezeigten Testergebnisse waren ein Anlass für einen Test am Bestand. Hierfür bot es sich an, dass die Öffentlichen Bibliotheken Berlins im Zuge der RFID-Einführung das Modell der Speicherung der UID im Bibliothekssystem gewählt haben. Für den Test wurde zeitnah die Sollliste erstellt, welche aus Mediennummer (UID), Signatur und Titel bestand.

Der Teilbestand mit 1580 Medien wurde mit den oben genannten Komponenten erfasst, wobei die große Reichweite der Antenne dazu führte, dass ungefähr 50 Transponder gleichzeitig erfasst werden konnten. Die Zeitdauer für den Durchlauf betrug rund 7 Minuten. Die bereits beschriebene Nacharbeit (Aufsuchen nicht detektierter Medien) nahm ca. 50 Minuten in Anspruch, wobei auch hier deutlich wurde, dass besonders Medien am Regalrand die Ursache für Erkennungsprobleme durch den Leser sind.

#	Anzahl Medien laut LMS	Mit RFID erfasst	nicht erfasst	Dauer Scannen	Dauer Nach-arbeit	Detektions-rate (%)
1	1580	1528	52	7	50	96,7

Tab. 4: Detektionsrate vom RFID-Handlesegerät bei UID-Inventur im VÖBB, Freihandaufstellung

Verglichen mit den Ergebnissen aus dem Jahr 2008, bei denen jeweils ältere RFID-Geräte und das Auslesen der Mediennummer zum Einsatz kamen, zeigt das Ergebnis des neuen Tests bereits Besserungen im Bereich der Erkennungsrate (Freihandaufstellung) und auch der Durchführungszeit.

Fazit

Die ersten durchgeführten Testinventuren in unserer Einrichtung waren damals in ihren Ergebnissen ziemlich ernüchternd. Faktoren die dazu beitrugen waren unter anderem die Vorbereitungsarbeiten für die Listenerstellung, der Listenim- und export bei den mobilen Geräten, die teilweise niedrigen Erkennungsraten sowie die Darstellung der Metadaten auf dem Gerät selbst. Hier zeigte sich ein großer Bedarf an einer geeigneteren Inventursoftware auf dem Gerät selbst bzw. nach einer Middleware, die fehlende Funktionen übernehmen konnte. Die Schwierigkeit einer geeigneten Lösung liegt hierbei sicherlich durch die Anzahl der verschiedenen LMS- und RFID-Anbieter begründet.

Die neuen Testergebnisse zeigen allerdings eine positive Entwicklung auf, was durch den Einsatz von angepasster Software und besserer Hardware (Lesegeräte, Antennen und Transponder) bedingt ist. Eine Erkennungsrate von knapp 96,7 Prozent im Freihandbereich, die durch eine größere Disziplin beim Scannen der Medien durchaus noch verbessert werden kann, zeigen was bei RFID-gestützten Inventuren möglich ist. Des Weiteren trägt auch der Ansatz der UID-Inventur zu einer Weiterentwicklung des Systems bei, welcher aber für Einrichtungen mit bestehendem RFID-System nur schwer umzusetzen ist.

Ein weiterer wichtiger Aspekt ist die Entwicklung von geeigneter Inventursoftware, was im folgenden Abschnitt, am Beispiel der Kooperation der UB Bielefeld mit der Firma Bibliotheca RFID Library Systems AG, vorgestellt werden soll.

Einführung eines Revisionstools an der UB Bielefeld

Rahmenbedingungen

Im Sommer 2011 wurden ca. 2 Millionen in Freihand stehende Bände in der Universitätsbibliothek Bielefeld mit RFID-Etiketten ausgestattet und konvertiert. Dabei wurde der Chip-Typ NXP SLI-X 54X86mm eingesetzt.

Digitale Medien, Zeitschriftenhefte und Magazinbestand erhielten keine RFID-Label. Die Etiketten wurden auf drei unterschiedlichen Höhen in den hinteren Buchdeckel geklebt, um eine Überlagerung der Etiketten zu verringern und so die Lesbarkeit zu verbessern.

Gleichzeitig zur Konvertierung wurde mit der RFID-Verbuchung an allen sieben Ausleihterminals begonnen.

Im November 2011 konnten dann zusätzlich vier Selbstverbucher an den beiden Hauptausgängen in den Bauteilen C und U in Betrieb genommen werden. Zu diesem Zeitpunkt wurden auch an allen sechs Fachbibliotheksausgängen die zuvor installierten smartgate™ 400 aktiviert.

Schon bei der Beantragung der Mittel für eine Buchsicherung mit RFID-Technik stand auch die Einführung eines Revisionstools im Focus. Zu beachten galt, dass im gesamten Freihandbereich Stahlregale verwendet werden, die immer als Handicap für das Auslesen von RFID-Etiketten galten.

Trotzdem blieb es ein erklärtes Ziel an der UB Bielefeld mit Einführung von RFID, einen Mehrwert – über die reine Buchsicherung, Stapelverbuchung und Selbstverbuchung hinaus – zu erreichen.

Gerade in einem großem Freihandbestand ist die Bestandskontrolle ein dauerhaftes Problem. Vermisste und verstellte Bücher können nur mit großem Aufwand bzw. gar nicht gefunden werden. Für eine umfassende Revision fehlt Zeit und Personal. Außerdem soll die Bibliothek dafür nicht geschlossen werden. Dies sind wesentliche Gründe zur Entwicklung eines Revisionstools.

Test der Lesegenauigkeit

Voraussetzung für eine funktionierende Revision und Ordnungskontrolle ist eine möglichst hohe Lesegenauigkeit. Daher legten wir von Projektbeginn an großen Wert auf ein leistungsfähiges Lesegerät.

Equipment:

In der 1. und 2. Phase wurde mit dem drahtlosen Akku-betriebenen Inventory Reader smartstock™ 100 von Bibliotheca gearbeitet. Die Auswertung erfolgte über ein PDA, das die eingelesenen Mediennummern auflistete, die Summe der eingelesenen Medien anzeigte und eine Dublettenkontrolle enthielt.

In der 3. Phase arbeiteten wir mit einem smartstock™ 110 mit USB-Anschluss an einem Laptop (Windows 7) mit ständiger Stromversorgung. Die eingesetzte neue smartstock-software von Bibliotheca stand uns als Arbeitsversion zur Verfügung und wurde gemeinsam mit Bibliotheca für uns konfiguriert.

1. Phase: Test der Lesemenge

In ersten Tests mit dem Inventory Reader smartstock™ 100 im Januar 2012 untersuchten wir die Lesegenauigkeit an größeren Bestandsmengen. In einem einzelnen, durchgehenden Lesevorgang wurden jeweils mehrere hundert Buchetiketten eingelesen. Anschließend zählten wir die Bände in den eingelesenen Regalbereichen und verglichen das jeweilige Ergebnis mit der Anzahl der eingelesenen Bände. Fehlten Bände, wurde in einem zweiten oder dritten Lesevorgang ermittelt, ob noch zusätzliche Etiketten erfasst werden konnten.

Diese Tests dienten auch der Verbesserung der Handhabung des Inventory Readers. Es stellte sich heraus, dass ein langsames wellenförmiges Bewegen von oben nach unten über die gesamte Buchrückenhöhe die beste Lesequote ergab. Ein schnelles Entlangführen der Antenne des Inventory Readers über die Mitte des Buchrückens brachte deutlich schlechtere Lesequoten.

2. Phase: Test der Standortreihenfolge

Im Unterschied zur 1. Phase wurden hier kleinere Bestandsmengen auf ihre genaue Standortreihenfolge hin untersucht. Dafür verglichen wir die Einlesereihenfolge jeder Mediennummer mit dem tatsächlichen Standort im Regal. Die eingelesene Mediennummernliste wurde hierfür exportiert und mit Hilfe eines im eigenen Hause entwickelten Programms mit Angabe der Signaturen visualisiert. Diese Tests dienten nochmals der Präzisierung der Lesegenauigkeit und der Verbesserung der Handhabung des Inventory Readers. So konnte festgestellt werden, dass – wie gewünscht – Bücher aus gegenüberliegenden Regalen bzw. von oberen und unteren Regalböden nicht mit eingelesen werden. Einleseprobleme ergaben sich jedoch an unseren doppelwangigen, metallenen Regalabgrenzungen. Etiketten im unteren Buchdeckelbereich wurden am Anfang eines Regalmeters manchmal nicht eingelesen. Entscheidend für das weitere Vorgehen waren auch die Ergebnisse zu den Abweichungen in der Reihenfolge der eingelesenen Medien zur Aufstellung im Regal.

Inventory-Reader-Test: 13.02.2012

Systemstelle OH415
Im Regal: 45 Bücher
Eingelesen: 42 Bücher
Die ersten Bücher im Regalmeter wurden vorgezogen.

Beim ersten Durchgang wurden 41 Bände eingelesen, im 2. Durchgang noch ein weiteres Buch (42).

Die nachträgliche Überprüfung der drei nicht eingelesen Titel ergab, dass ein Etikett nicht konvertiert war.

Regal	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Eingelesene Reihenfolge	1	2	42	4	3	5	6	7	8	10	9	14	13	11	12	15	21	16	18	17	22	19	20	29	31	24	30	23

Regal	29	302	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
Eingelesene Reihenfolge	25	–	–	–	28	26	27	32	34	33	36	35	40	38	37	39	41

Aus dieser – der Funktechnik geschuldeten – Abweichung der Lesereihenfolge ließ sich ableiten, dass eine Regalordnungskontrolle nur über einen gewissen Toleranzbereich hinaus möglich ist. Gravierende Versteller sind jedoch gut zu ermitteln.

Im Zusammenhang mit der Lesegenauigkeit von Inventory-Readern wird immer nach Prozentzahlen zur Lesegenauigkeit gefragt. Unsere Ergebnisse schwankten je nach Arbeitsweise und Bestandsdichte zwischen 95 % und 100 %. Trotz sehr konzentrierten Arbeitens ließ sich eine gewisse Fehlquote jedoch nicht vermeiden und auch nicht immer schlüssig erklären.

Praxistauglichkeit und Anwendungsszenarien

Abb. K1: Einsatz des Smartstock in der UB Bielefeld

1. Revision am systematisch aufgestellten Freihandbestand

In dieser 3. Phase wurde der Online-Abgleich mit dem SISIS-Ausleihsystem (LMS) entwickelt und getestet. Das Programm für das eingesetzte Auswertungstool wurde an der UB Bielefeld entwickelt (Entwicklerkontakt: Friedrich Summann, E-Mail: friedrich.summann@uni-bielefeld.de).

Im folgenden Abschnitt wird die derzeitige Vorgehensweise beschrieben:

An einer speziellen Systemstelle wird zunächst der Bestand mit dem smartstock™ 110 eingelesen. Problemzonen werden beachtet, z. B. werden die ersten beiden Bücher an doppelwangigen Regalanfängen vorgezogen und dann eingelesen. Bei einer Vielzahl von dünnen, insbesondere mit Metallklammern gehefteten Broschüren, wird die Antenne auch zwischen die Bücher geschoben, um den Lesevorgang zu erleichtern.

Anschließend wird die mit der von Bibliotheca angebotenen smartstock-software erzeugte Datei mit Mediennummern auf einem Laptop per W-LAN in ein Netzlaufwerk kopiert. Über eine in Bielefeld entwickelte Weboberfläche wird der aktuelle Bestand an der zu kontrollierenden Systemstelle per W-LAN abgefragt und mit der eingelesenen Datei online abgeglichen.

Da alle im LMS an einer Systemstelle verzeichneten Bände mit der am Regal eingelesenen Mediennummernliste abgeprüft werden, ergibt sich eine hundertprozentige Kontrolle der Systemstelle.

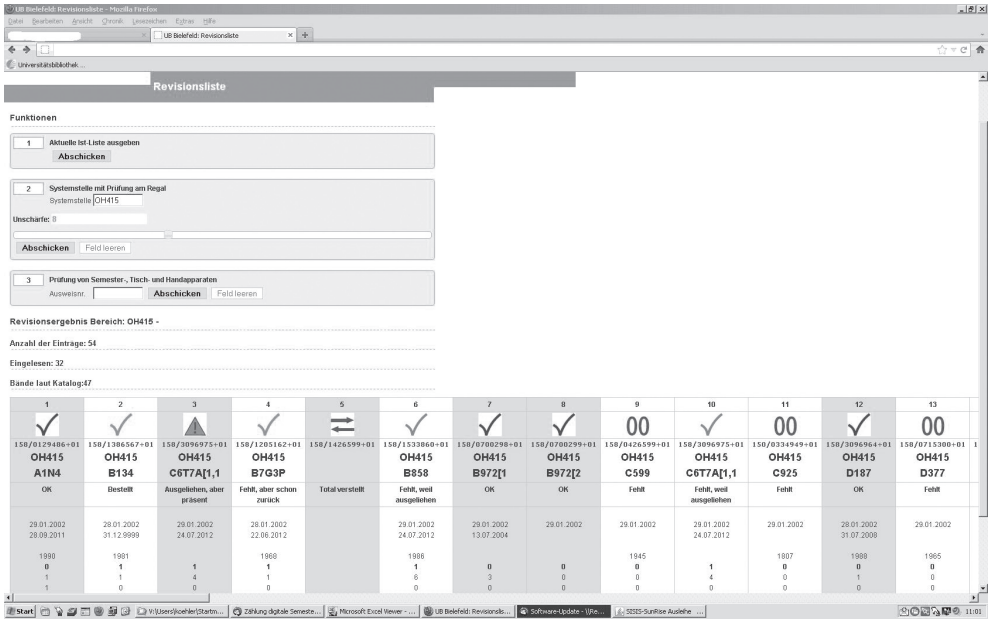


Abb. K2: Revisionstool

Die Abbildung gibt die Auswertung an der Systemstelle OH415 wieder:

- Grau unterlegte Einträge (s. Nr. 1,3,5,7,8, und 12) entstammen der mit der smartstock-software eingelesenen Datei mit Mediennummern (Ist-Liste).
- Weiß unterlegte Einträge (s. Nr. 2,4,6,9-11 und 13) wurden aus dem LMS abgefragt.
- Ein grüner Haken kennzeichnet Bände, die an der richtigen Stelle im Regal stehen.
- Ein grauer Haken wird ausgegeben, wenn ein Titel entliehen ist und daher nicht im Regal stehen kann.
- Steht ein *verbuchter* Titel im Regal, wird dies mit einem *Warndreieck* inkl. Ausrufungszeichen (s. Eintrag 3) signalisiert.
- Mit einem orangefarbenen Haken gekennzeichnete Einträge beschreiben Bücher, die fehlen, weil sie im Reservierungsregal stehen (s. Eintrag 2), soeben erst zurückgegeben (s. Eintrag 4) oder gerade eingearbeitet wurden.
- Als fehlend (mit 00) gekennzeichnete Medien können tatsächlich am Standort fehlen, kein Etikett haben, nicht oder falsch konvertiert sein oder bei der Revision nicht eingelesen worden sein. Diese Fälle sind individuell zu überprüfen. Hilfreich für die Suche nach fehlenden Büchern ist der Link über die Mediennummer zur Titelaufnahme im Bibliothekskatalog. Die Kollegen schätzen besonders die dort enthaltene Abbildung des Covers, die natürlich bei der Suche im Regal sehr hilfreich ist.
- Mit einem roten Wechselpfeil (s. Eintrag 5) werden grob verstellte Bücher markiert. Dies gilt für Bücher, die nicht dem unter Funktion 2 abgefragten Systemstellenbereich entstammen oder, wie in unserem Beispiel, nicht mit der eingelesenen Mediennummer im LMS zu finden sind. Daher kann hier auch keine Ausgabe der Systemstelle erfolgen. In diesem Fall muss nach der Fehlerquelle gesucht und neu konvertiert werden. Zunächst muss natürlich das Buch im Regal gesucht werden. Hierfür kann auch die smartstock-software von Bibliotheca hilfreich sein. Mit der Funktion »Search for Missing Item Numbers« lassen sich einzelne oder mehrere Titel anhand ihrer Mediennummer mit dem Inventory Reader suchen. Beim Einlesen der gesuchten Mediennummern ertönt – auch wiederholt – ein akustisches Signal.
- Die Datumsangaben geben das Aufnahmedatum und das Leihfristende bzw. das letzte Rückgabedatum wieder. Zusätzlich werden das Erscheinungsjahr und die Ausleihzähler ausgewertet.

Je nach Bestandsdichte und dem Aufkommen von Mehrfachexemplaren mit identischer Signatur lässt sich ein Unschärfeparameter eingeben, der eine variable Verstellertoleranz ermöglicht und gleichzeitig die Leseunschärfe, die in Phase 2 beschrieben wurde, berücksichtigt. Dieser Unschärfewert gibt an, wie viele Stellen ein Buch von seiner Sollstelle im Regal abweichen darf, ohne als Versteller gekennzeichnet zu werden. In Abbildung 2 wurde die Unschärfe mit 8 eingegeben. Mit diesem Wert 8 wurde in unserem Beispiel kein Versteller gefunden. Solche Versteller würden mit einem grünem Wechselpfeil gekennzeichnet.

2. Revision eines Semesterapparates

Mit der Funktion 3 unseres Auswertungstools lassen sich besondere Aufstellungsformen in Freihandbereichen überprüfen. Wir verwenden diese Funktion zur Zeit für die Überprüfung von Semesterapparatsaufstellungen.

Die Handhabung des Inventory-Readers gleicht der Vorgehensweise an einer Systemstelle: Nach dem Einlesen mit dem smartstock am Regal und dem Erzeugen einer Mediennummernliste mit der smartstock-software läßt sich mit dem Bielefelder Auswertungstool dann auch ein Benutzerkonto überprüfen.

Unter der Funktion 3 aus Abbildung 2K: »Prüfung von Semester-, Tisch- und Handapparaten« wird nach Eingabe der Benutzernummer eines Semesterapparatskontos die eingelesene Mediennummernliste mit dem Benutzerkonto abgeglichen und auf Vollständigkeit, Versteller etc. überprüft.

Verbleibende Defizite:

Trotz des hundertprozentigen Abgleichs eines Benutzerkontos oder einer Systemstelle können folgende Unschärfen bestehen bleiben: Wird ein Titel nicht eingelesen *und* ist gleichzeitig ein grober Versteller (also nicht aus dem abgefragten Systemstellenbereich oder einem Benutzerkonto) kann er nicht vom Auswertungstool erfasst werden. Folgende Gründe sind möglich:
- verbleibende Fehlquote in Höhe von 5 %
- kein Etikett
- mit Etikett, aber nicht konvertiert
- defektes Etikett

Dieses Defizit lässt sich nur durch manuelles Zählen der Bände im Regal beheben. Das ist jedoch bei unserem Bestand von 2 Millionen Bänden nicht sinnvoll.

Fazit und zukünftiger Einsatz

Mit dem Revisionstool kann man während des laufenden Betriebs die Bestände am Regal online überprüfen. Dies gilt sowohl für systematisch aufgestellte Bestände, als auch für Medien, die für besondere Aufstellungsformen verbucht sind.

Mehrere Inventory-Reader können gleichzeitig eingesetzt werden. Wir planen den Einsatz von sieben smartstock™ 100 im Routinebetrieb.

Die Revisionsarbeiten verlangen ein konzentriertes Vorgehen und eine genaue Kenntnis des LMS und der jeweiligen Aufstellungsbesonderheiten. Je nach Ordnungszustand im Regal ist dieser Arbeitsanteil der Auswertung um ein Vielfaches höher als der des reinen Einlesens. So kann die Bearbeitung von zwei Buchregalmetern bis zu einer halben Stunde dauern, während hierfür der Einlesevorgang selbst im Schnitt nur ca. 30 Sekunden dauert.

Es kann aber keine genaue Aussage über die Gesamtdauer einer Revision gemacht werden. Der erste Revisionsdurchgang ist wahrscheinlich der Aufwendigste. Hier werden in Bielefeld Bestände abgeglichen, die bereits 50 Jahre in Freihand stehen können. Daher gibt es eine Vielzahl an Fehlerquellen wie z. B. Beschriftungs-, Buchungs- und Konvertierungsfehler, die bei einem zweiten Durchgang dann bereinigt sein werden.

Literatur und Internetquellen

[1] Bibliotheca.com (2012). Produktspezifikation Smartstock 100/110 http://www.bibliotheca.com/1/index.php/de/unsere-produkte/mitarbeiterl%C3%B6sungen/smartstock%E2%84%A2-100-110

[2] Fortune, Mick. (2012). RFID Survey 2012 – Equipment reliability http://www.libraryrfid.co.uk/equipreliability.html

[3] Kern, Christian. (2006). Anwendung von RFID-Systemen. Heidelberg: Springer Verlag Berlin

[4] Finkenzeller, Klaus. (2008). RFID Handbuch München: Carl Hanser Verlag

[5] Deutsches Institut für Normung e.V. / Normenausschuss Bibliotheks- und Dokumentationswesen. (Ausgabe 2009-11). DIN-Fachbericht 13:2009-11, Bau- und Nutzungsplanung von Bibliotheken und Archiven. Berlin: Beuth Verlag

[6] Philips Semiconductors (Hrsg.). (2003). I-CODE SLI Label IC, functional specification Data (rev. 3.0)

[7] ISO/IEC. (2009). Identifikationskarten – Kontaktlose Chipkarten – Vicinity Cards – Teil 3: Antikollisionsverfahren und Übertragungsprotokoll. Genf (ISO 15693-3)

[8] ISO. (2010). Information and documentation – RFID in libraries/3 – Fixed length encoding. Genf (ISO 28560-3)

Die zitierten Internetquellen wurden zuletzt am 04.10.2012 aufgerufen.

Inventory – an innovative area of research and implementation of RFID technology

Michał Grabia, Tomasz Janiak

Since its inception, the Institute of Logistics and Warehousing in Poznan has focused its research potential issues related to logistics and storage in a broad sense. One of the most common processes in this area, which we can actually meet both in business environments and in every household, is inventory.

A »physical« inventory of available material resources and registration of results of this activity is a process that dates back to the ancient past. According to archaeologists, the clay tablet considered Europe's oldest written text, found in the ruins of the Mycenaean buildings in a small Greek village Iklaina on Peloponnese, is the list of someone's property, which was probably made between 1450-1350 BC. Similar artefacts have also been found in the ruins of other ancient cultures around the world.

In the past few years, the inventory process has undergone a major evolution, which we generally owe exclusively to the development of automatic identification technologies. Inventory activities, which were originally performed based on visual identification and manual registration of results on a sheet of paper, have been improved through the introduction of barcodes and portable scanners/terminals directly connected to the data collection systems. In addition, in recent years the world has seen this process subjected to further improvements through the introduction of even more advanced automatic identification techniques based on radio waves – RFID.

The area of potential applications of RFID technology is very wide, but unlike barcodes, the application of this technique also has some limitations. Not all of the objects and environments are equally friendly to radio waves. Placing RFID tags on containers with liquids or on metal objects or even the installation of the system in areas with harsh environmental conditions (such as interference from electric motors, collisions with other RFID systems or with a large number of objects made of metal) can sometimes be a problem.

Accordingly, in recent years, there is a significant increase in the number of implementations, but only in certain industries, in which problems with the implementation of RFID are practically absent or minimal. The group of such areas, which were the first to take the challenge of implementing this technology, includes libraries and archives.

Libraries were the one of the first institutions to initiate the process of adapting ADC technology to their needs. At the moment, a lot of libraries in Europe and around the world use the ability to identify existing resources based on the reading of RFID tags placed on the books. So far, most of them concentrated on the use of RFID technology operating in high frequency – HF. Recently, however, we hear more and more often about the implementation of new solutions based on the UHF band.

The reason for this seems to be obvious. The first UHF solutions were not perfect and had many weaknesses. The effectiveness of these systems left much to be desired. In addition, there was also no possibility of an easy use of RFID tags in both the management of books and magazines (such as renting, returns, etc.) while simultaneously carrying out anti-theft EAS functions (Electronic Article Surveillance).

Recent RFID solutions no longer have this problem, and additionally due to the shape of the tag, they allow for more effective securing of books. An oblong, relatively narrow RFID UHF transponder can be pasted between the pages right at the back of the book in such a way that finding it may be a problem even for the person who placed it there. Inability to locate the tag also protects the book against intrusion of the reader and ultimately an attempt of its theft.

Also in the area of inventory, the new technology has introduced new opportunities, which, in comparison with both the classical method (visual identification combined with manual registration on sheets of paper) or using barcodes allows for achieving a completely new quality, especially in regard to the time required to perform the actual physical inventory, which in the case of RFID applications has been significantly reduced, and results from the fact of not having to see the label placed on the marked object.

As part of research carried out at the Institute of Logistics and Warehousing, the measurements of time required to complete the inventory were performed using two different techniques of automatic identification. An independent team of ILiM employees marked the selected objects in randomly selected rooms of the Institute. Subsequently, four independent testers carried out a physical inventory in all these rooms by using two selected identification techniques (barcode and RFID). Due to the need to eliminate the possibility of remembering which objects have been marked, each tester first conducted an inventory only using barcodes. It was only after the measurement of time in all the rooms that the test was repeated with the use of radio frequency technology for the identification of objects – RFID.

The obtained results clearly confirm that the use of RFID will significantly reduce the time needed for the implementation of inventory activities. The study shows that the inventory based on RFID may be performed even up to 80 % faster than using barcodes [Tab. 1].

No. Meas.	Number of tagged objects	ADC technology	Inventory time by individual testers [mm:ss]				Average inventory time [mm:ss]	Standard deviation	Profit	Average single object scanning time [mm: ss]
			Person 1	Person 2	Person 3	Person 4				
A	61	Barcodes	07:52.0	07:35.0	07:27.0	07:29.0	07:35.8	0.000131	80 %	00:07.5
		RFID	01:06.0	02:07.0	01:13.0	01:35.0	01:30.3	0.000318		00:01.5
B	47	Barcodes	06:27.0	06:15.0	07:28.0	06:45.0	06:43.8	0.000370	75 %	00:08.6
		RFID	01:37.0	01:47.0	01:29.0	01:45.0	01:39.5	0.000095		00:02.1
C	30	Barcodes	04:19.0	03:23.0	03:06.0	02:49.0	03:24.2	0.000452	71 %	00:06.8
		RFID	01:30.0	00:45.0	00:53.0	00:48.0	00:59.0	0.000242		00:02.0

No. Meas.	Number of tagged objects	ADC technology	Inventory time by individual testers [mm:ss]				Average inventory time [mm:ss]	Standard deviation	Profit	Average single object scanning time [mm: ss]
			Person 1	Person 2	Person 3	Person 4				
D	16	Barcodes	01:49.0	02:27.0	02:35.0	02:42.0	02:23.3	0.000274	77 %	00:09.0
		RFID	00:30.0	00:50.0	00:23.0	00:29.0	00:33.0	0.000136		00:02.1
E	20	Barcodes	02:13.0	01:24.0	02:16.0	02:05.0	01:59.5	0.000279	60 %	00:06.0
		RFID	00:30.0	00:44.0	01:00.0	00:58.0	00:48.0	0.000161		00:02.4
F	8	Barcodes	00:30.0	00:39.0	01:10.0	00:33.0	00:43.0	0.000213	60 %	00:05.4
		RFID	00:10.0	00:13.0	00:15.0	00:31.0	00:17.3	0.000109		00:02.2

Tab. 1: The results of the measurements of inventory time

In addition, as part of the study, tests were carried out on the dependence of the time needed to carry out an inventory on the number of objects tagged (test rooms contained different numbers of tagged objects). The results of the study are clear and allow for proposing a thesis that the effect of time reduction of an inventory is greater with the increase in the number of tagged objects. As a result, we could be tempted to say that the higher the number of tagged objects, the shorter the physical inventory using RFID, in comparison to the use of classical barcodes [Fig. 1].

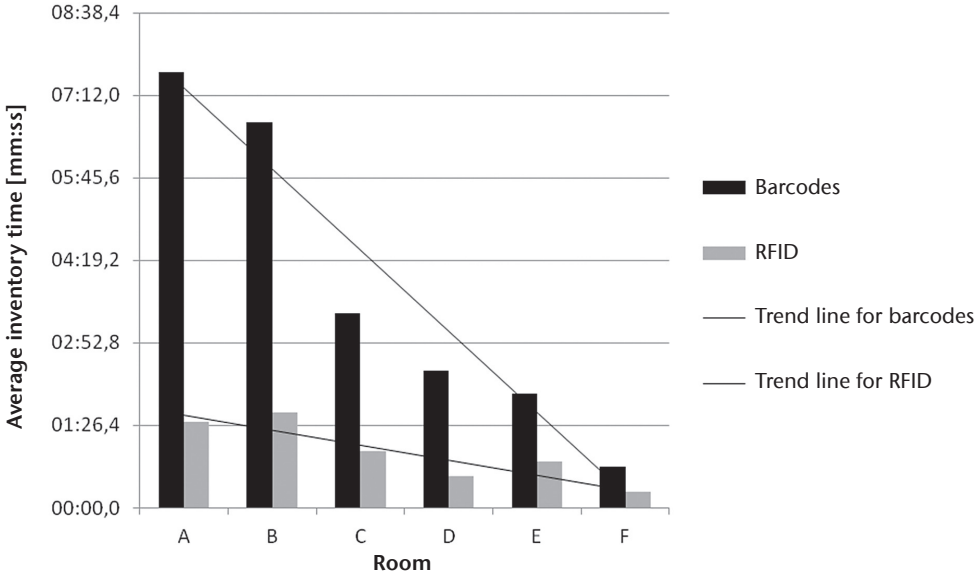


Fig. 1 Comparison of the duration of the inventory process carried out in selected test rooms using two different techniques of automatic identification (barcodes and RFID)

The results obtained were the basis to undertake further work at the ILiM on the potential use of RFID technology in the inventory process. In the course of the »Use Case Analysis« carried out on the use of RFID in inventory, we identified a number of situations that have never been taken into account (in the context of the use of classical methods or barcodes) and which may occur only in the case of RFID applications [Tab. 2].

No.	Data on the terminal application		Factual circumstances	Comment	Reaction	
	Tag reading	Expected	Object present?		Reaction of the application	User reaction
1	No	No	No	Typical situation, the object is not there.	None	None
2	No	No	Yes	Tag damaged, the object has been moved	None	Entry in the notebook
3	No	Yes	No	Typical situation, the object has been moved	On the list of expected objects	None
4	No	Yes	Yes	Tag damaged	On the list of expected objects	Entry in the notebook
5	Yes	No	No	Tag reading through the wall	On the list of redundant objects	Cancelled reading
6	Yes	No	Yes	Typical situation, the object has been moved	On the list of redundant objects	None
7	Yes	Yes	No	Object has been moved, reading through the wall	Removal from the list of expected objects	Cancelling the reading
8	Yes	Yes	Yes	Typical situation.	Removal from the list of expected objects	None

Tab. 2: Identified use cases for the inventory application using RFID technology

Of particular interest is a situation in which the person performing the physical inventory accidentally identifies an object located in another room (through the wall). Until now, such an event would practically never occur. The system solution created at the ILiM would therefore have to not only allow handling such an unusual situation but at the same time meet the other requirements identified by the persons who normally carry out inventories. The table below lists the additional features of the system created, based on interviews with persons responsible for carrying out inventories [Tab. 3].

No.	Requirement	Justification
1	Physical inventory should be carried out using just the terminal.	No need to use (and carry) additional devices, such as notebook.
2	The terminal should handle barcodes and RFID.	Ability to identify an object in case of problems with the identification of RFID tags.
3	The terminal should work without being connected to WLAN.	Ability to conduct an inventory in areas without wireless access.
4	Terminals should synchronise via WLAN whenever possible.	The ability to coordinate the inventory, for example, warning against inventorying the same room twice.
5	The terminal should operate as far as possible without a stylus.	More comfortable to use.
6	Objects can be described using definable attributes.	Assigning objects (including fixed assets) to individual organisational units, people, or the ability to create own vocabulary of criteria.
7	The system should allow for the storage of photographs of tagged objects.	More comfortable to use in case of problems with finding an object based on its name or description.

Tab. 3: List of inventory system requirements created on the basis of interviews with persons carrying out the inventory.

The requirements collected become the basis for defining the system architecture. The inventory process makes it necessary to implement an application for computers, allowing for management of the physical inventory, and a terminal application, running on

handheld RFID readers. To make these two applications independent of each other, that is to allow the operation of one without the other, as well as the simultaneous operation of multiple instances of the application, it was decided to add an intermediate layer consists of a database together with mechanisms for sharing and synchronising data [Fig. 2]. The intermediate layer is installed on any computer (or in case of heavy load, on the appropriate server) and is activated for the duration of inventory process.

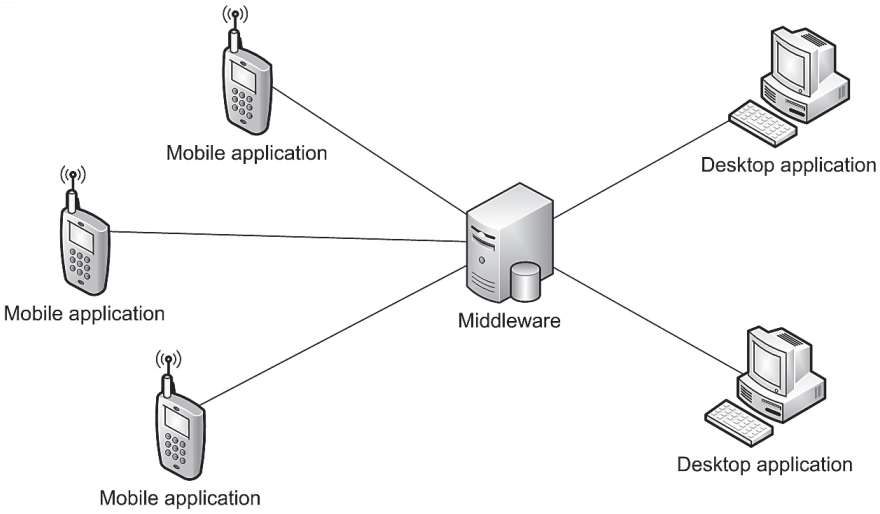


Fig. 2: Diagram of the system architecture.

In addition to functional requirements that define the utility value of a component of the IT inventory system, a reconnaissance of the RFID technology itself was carried out as part of the study. Tests of selected RFID tags were conducted, in the context of their applicability to tag the inventoried objects. The following transponders were chosen for testing:

1. UHF Rafsec G2 242_1 20 mm x 40 mm.
2. UHF Rafsec G2 163_2 56 mm x 86 mm.
3. UPM Rafsec PD70_18_6.
4. Alien 1800047.
5. Rafsec G2 100 mm x 15 mm.
6. Rafsec G2 100 mm x 20 mm.

Tests of the reading range were performed using substrate inert to radio frequency (in this case it was a wooden substrate) in horizontal and vertical orientation, with the manual AT570 reader and the stationary Impinj reader (for comparison). The test results are shown in the table below [Tab. 4]. It is worth noting that the range of the manual reader is significantly smaller than the range of a desktop reader, which is further supported by the data contained in the specifications (maximum theoretical range of the MC9090-G reader is about 3 m). This is related to the limited power of mobile devices resulting from the need to comply with the ETSI EN 300 220 standard, and the fact of their limited energy resources (battery power supply).

No.	Manufacturer	Name/Type	Tag dimensions	Label dimensions	Horizontally AT570	AT570 vertically	Impinj horizontally	Impinj vertically
			[mm]	[mm]	[cm]	[cm]	[cm]	[cm]
1	Rafsec	G2 242_1	20 x 40	20 x 40	10	10	40	40
2	Rafsec	G2 163_2	56 x 86	56 x 86	230	260	500	540
3	Rafsec	PD70_18_6	15 x 96	15 x 96	160	140	490	600
4	Alien	1800047	15 x 100	108 x 178	220	250	680	670
5	Rafsec	G2	15 x 100	108 x 178	230	170	480	420
6	Rafsec	G2	20 x 100	108 x 178	160	230	540	500

Tab. 4: Results of tests on selected RFID tags.

The pool of tested RFID tags is defined both on the basis of the results of the reconnaissance as well as the results of previous studies of RFID technology, conducted at the ILiM. In the course of the study, we selected both tags possible to be applied in the form of paper labels as well as universal transponders, operating efficiently regardless of the substrate material on which are placed [Tab. 5].

No.	Manufacturer	Name/Type	Dimensions	Wood	Metal	Glass	Cardboard	Polyethylene	Air
			[mm]	[cm]	[cm]	[cm]	[cm]	[cm]	[cm]
1	OmniID	Flex	97/21/6	110	130	240	110	100	70
2	OmniID	Prox	55/16/8	60	80	70	55	55	40

Tab. 5: Results of tests on selected universal RFID tags.

Based on the results of the tests performed, we decided to select 4 types of tags for the tests of the inventory system. The selection took into account both the achieved reading range of the tags, as well as their size and the number of available samples:

1. UHF Rafsec G2 163_2 56 mm x 86 mm.
2. Rafsec G2 100 mm x 15 mm.
3. UPM Raflatac Dog Bone 97 mm x 27 mm.
4. OmniID Flex 97 mm x 21 mm

First, it was decided to conduct an inventory of objects tagged only with tags placed underneath self-adhesive labels, so-called Smart Labels. This solution has certain advantages, such as:

- The possibility of printing over – as in the case of conventional labels.
- Low cost of the tag – depending on the model, several euro-cents apiece.
- High availability – a large variety of models offered by different suppliers.
- Small thickness – the label has dimensions similar to the dimensions of an ordinary labels without an RFID tag.

The tests confirmed that the main drawback of tags placed on labels is the high impact of the substrate on the effectiveness of their reading. Labels work well on material neutral for radio waves, such as wood, paper or plastic, but in practice they do not work at all when placed on a metal surface. For this reason, it is necessary to choose a different approach for the identification of metal objects. The analysis showed that, in principle, it is possible to take several courses of action:

– More expensive tags dedicated to metal (tests were carried out using selected OmniID Flex tags).
– Separation of tags on labels from the substrate using a neutral layer, such as a cardboard backing.
– Placing tags on labels next to the tagged objects.
– Identification using barcodes only.

Each of these directions is always applicable and the decision to choose one of them, in the opinion of the research team, should always be left to the institution implementing the inventory solution being developed. One of such institutions, where a pilot implementation of the developed solution is currently taking place, is the Raczynski Library, operating in Poznan (Poland) since the beginning of the nineteenth century.

In the course of implementation, the library's fixed assets will be tagged with labels printed with a barcode and an RFID tag with EPC number programmed according to the GIAI standard (Global Individual Asset Identifier). A physical inventory will be carried out using a mobile terminal equipped with ATID 870 terminal equipped with a barcode reader and an RFID module. The inventory process will be started from the data synchronisation between the fixed assets database and the terminal, using a wireless network. In this way, the person conducting the inventory will be sure that the most recent data are used. Then, assets will be inventoried by reading RFID tags or barcodes printed on labels (a decision was made in the first phase of implementation to use barcode labels to tag all the objects made of metal). The solution implemented at the Raczynski Library allows the person performing the inventory to inspect the list of read, expected and redundant assets at any time, which greatly speeds up the work and allows for reducing the number of possible errors. After completing the inventory, the list of IDs read is sent to the system's central database. This allows for both viewing the inventory data from a computer, on which the desktop application is installed, generating reports on shortages, surpluses, inventory sheets, etc. in accordance with pre-defined templates. It also allows for exporting the results of the inventory to the financial and accounting application in order to make the necessary settlements.

The comprehensive software and hardware solution developed at the Institute of Logistics and Warehousing also has a number of other interesting features. In the desktop application, the following possibilities have been introduced, as expected by future users:
– User authentication [Fig. 3],
– Defining groups of users with different privileges,
– Work on multiple computers at the same time,
– Import of data from external sources (e.g. via Excel files, XML files, etc),
– Printing labels for assets and programming RFID tags,
– Editing fixed assets [Fig. 4],
– Reporting of inventories carried out [Fig. 5],
– Return to archival inventories,
– Adding attributes to fixed assets and their dictionaries,

Fig. 3: Login screen of the computer application

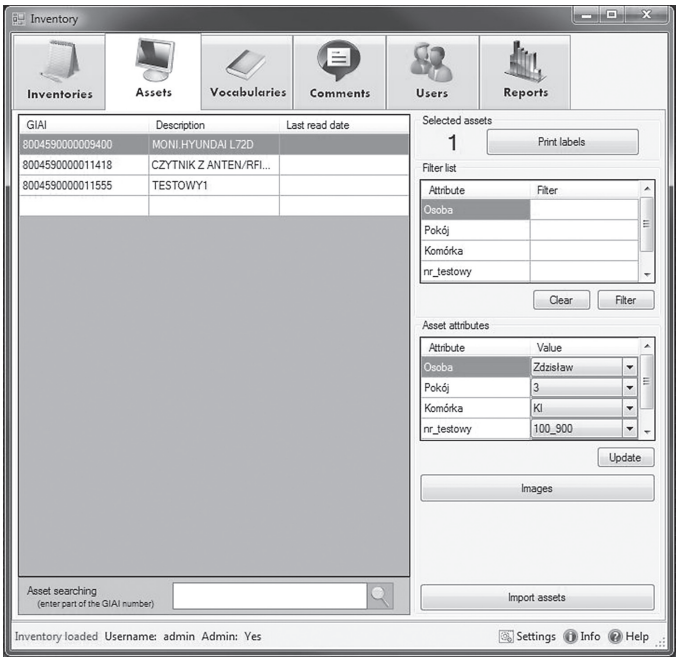


Fig. 4: Asset viewing screen in the computer application

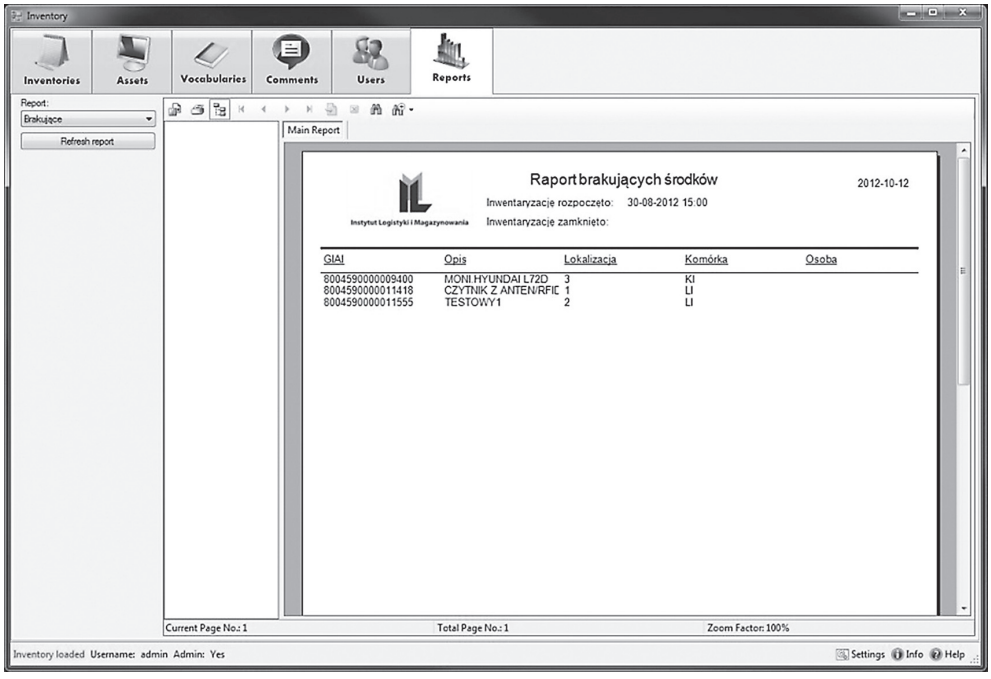


Fig. 5: Reporting screen in the computer application

A number of specific features, which have been implemented as expected have also been identified in the terminal. The most important ones are:
- User authentication;
- Wireless sync with the current database of fixed assets;
- Identification of the selected fixed asset based on the reading of its barcode or RFID tag;
- Displaying detailed information about the selected fixed assets;
- Viewing pictures of fixed assets;
- Editing the attributes of fixed assets;
- Editing the attributes of location of fixed assets;
- Adding comments;
- Programming RFID tags;
- Search of an asset based on its number (for RFID tags only);
- Support for any terminal with Windows CE or Windows Mobile.

The combination of the two software components with hardware (RFID tags, terminals and printers) selected during the tests allows users to effectively and efficiently carry out all inventory processes. In libraries, this can apply to the fixed assets held and ultimately also books and magazines. The condition for such full use of the application is the use of the RFID UHF solution in the given library and not, as is quite often the case – the HF solution. Maintaining compatibility of the two solutions allows for much more efficient use of the solution developed at the ILiM and significantly strengthening the benefits of its implementation, which can include effects such as:
- Reducing inventory costs by shortening the time of its conduct;
- Shortening the duration of the inventory by up to four times using RFID tagged labels compared to markings with barcode alone;
- Reducing the number of people needed to carry out the inventory;
- Aesthetic marking of fixed assets or the possibility of hidden markings;
- The ability to quickly make changes to the status of the premises;
- Easy access to information and generating reports on the status of property;
- The possibility of frequent inventories.

Summary

The development of automatic identification technology has become an important stimulus for the improvement of the inventory process in a variety of industries. From the standpoint of practical applications, the universality of the described solution, which uses RFID technology, should be emphasised. In libraries, RFID-assisted inventory may be applied not only to the fixed assets held, but also the stored media (books, magazines, CDs). Pilot implementation of the application in one of the largest Polish libraries indicates a forward-looking nature of this solution and the benefits of effective time management. The use of RFID technology in libraries and archives allows for speeding up the work and reducing the number of mistakes, as evidenced by the tests conducted by the Institute of Logistics and Warehousing, confirming the reduced inventory times by up to 80 % compared to the inventory with the use of barcodes.

Schnittstelle für Selbstbedienungsautomaten in RFID-Bibliotheken

Vergleich der Schnittstellen SIP2 und NCIP

Barbara Michaelis

In RFID-Bibliotheken erfolgt die Kommunikation zwischen Selbstbedienungsautomat und Bibliothekssystem mittels standardisierter Protokolle. Zurzeit sind vor allem die Protokolle SIP2 und NCIP im Einsatz. Diese unterscheiden sich im strukturellen Aufbau und im Bereich der Definitionen grundlegend voneinander. Daraus ergeben sich wesentliche Einflüsse auf den Aufwand für die Installation und Wartung der Schnittstelle zwischen Selbstbedienungsautomaten und Bibliothekssystem.

Kommunikation zwischen Selbstbedienungsautomat und LMS (Library Management System)

Für den Einsatz von Selbstverbuchungsgeräten muss die Frage der Kommunikation zwischen diesem und dem Bibliothekssystem (LMS) gelöst werden. Dabei ist es unerheblich, mit welchen Lesevorgängen (Barcode, RFID oder Bilderkennung) gearbeitet wird. Die Geräte arbeiten heutzutage vorwiegend auf der Grundlage der RFID-Technologie. Selbstverbuchungsgeräte besitzen jeweils Programme für die Lösung ihrer Aufgaben. Ein integriertes Bibliothekssystem bedient eine Vielzahl von Arbeitsplätzen und Geräten. Die notwendigen Prozesse werden zentral auf Servern verwaltet. So ist es erforderlich, die Kommunikation von einem Selbstbedienungsgerät zur Serverapplikation des LMS zu gewährleisten. Das kann individuell gelöst werden. Der Nachteil individueller Lösungen besteht immer darin, dass diese für andere Konstellationen nicht anwendbar sind. So haben sich für die Kommunikation im bibliothekarischen Bereich seit langem verschiedene Protokolle entwickelt. Damit wird die Unabhängigkeit zwischen den Herstellern der Automaten und der Bibliothekssysteme weitgehend gewährleistet.

Damit Protokolle breite Anwendungsmöglichkeiten finden und auch über längere Zeiträume verwendbar sind, sollten sie folgende Eigenschaften besitzen:
- eindeutige Regeln und Definitionen
- Unterstützung sämtlicher Erfordernisse
- Stabilität
- Flexibilität und Weiterentwicklung

Mängel oder Lücken werden von den Anwendern selbst durch Modifizierung ausgeglichen. Damit entstehen Lösungen, die für andere Applikationen in dieser Form nicht mehr nutzbar sind. Beide Partner müssen sich immer wieder mit diesen Modifikationen auseinandersetzen. Damit erhöhen sich der Aufwand für die Hersteller sowie die Kosten für die Bibliotheken.

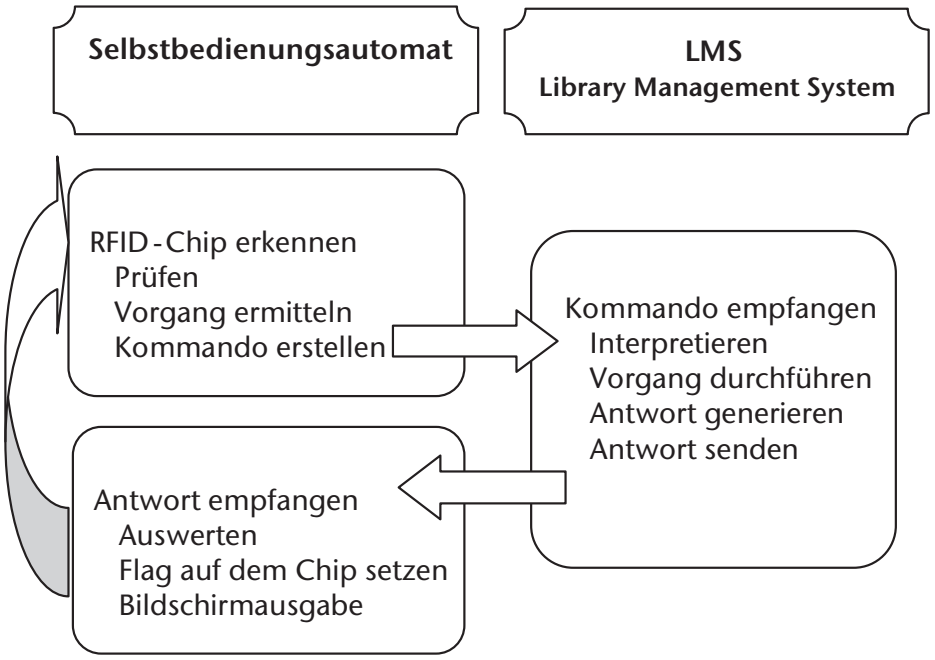


Abb. 1: Kommunikation: RFID-Selbstbedienungsautomat -Bibliothekssystem

Welche Kommunikationsprotokolle existieren bereits?

Ein Standard für die Selbstverbuchung wurde bereits 1997 von 3M entwickelt. Dieser Standard -SIP (Standard Interchange Protocol) -wurde dann von vielen Bibliotheken eingesetzt und ist als SIP2 (3M ™ Standard Interchange Protocol Version 2.00) heute noch das am meisten verwendete Protokoll. Es wird fortlaufend weiter entwickelt.

Im Zuge der Entwicklung Web-basierter Bibliotheken und des ILL (Interlibrary Loan) entstand die Notwendigkeit des Austauschs von Daten von Bibliotheken, Benutzern und Exemplaren sowie auch der Ausführung von Operationen für Benutzer und Exemplare in anderen Bibliotheken. Auf der Grundlage des bereits vorhandenen SIP2-Protokolls wurde für die neuen Herausforderungen das NISO Circulation Interchange Protocol (NCIP-Z39.83) entwickelt. Die erste Version entstand im Jahre 2002. Dieses umfassende Protokoll beinhaltet auch die Funktionen, die für die Kommunikation zwischen Selbstverbuchern und LMS notwendig sind. Die aktuelle Version ist aus dem Jahr 2008.

Ein weiteres Protokoll ist SLNP (Simple Library Network Protocol) der Firma SISIS. Dieses wird vorwiegend in SISIS-SunRise-Anwendungspaketen für Fernleihserver in deutschen Bibliotheksverbünden eingesetzt und ist vom Funktionsumfang für die Selbstverbuchung nicht so gut geeignet.

Der Einsatz von API-Schnittstellen (application programming interface) ist natürlich auch denkbar. Hierbei sind dann jedoch umfassende individuelle Vereinbarungen notwendig.

Grundlagen der Protokolle SIP2 und NCIP

Der Verbindungsaufbau für einen Prozess kann für beide Protokolle über TCP/IP (Transmission Control Protocol/ Internet Protocol**)** erfolgen. Die Verbindung über Web-Services (http bzw. https) ist nur für NCIP möglich. Eine verschlüsselte Verbindung über https ist somit nur bei Verwendung von NCIP möglich.

Die Verbindung selbst ist verbindungsorientiert (Connection oriented). Damit entstehen zeitweise Interaktionen zwischen den Partnern in Realzeit. Das Selbstbedienungsgerät setzt einen Request (Anfrage) ab und das LMS beantwortet den Request sofort.

Die Requests werden prozessunabhängig ausgeführt, d. h. jede Interaktion ist unabhängig von vorigen Aktionen. Damit kann eine Verbindung ohne nachfolgende Probleme nach jeder Interaktion enden. Für eine weitere Interaktion wird dann eine neue Verbindung automatisch aufgebaut.

Protokollsprachen

SIP2

Hier werden Request und Response (Antwort) in strukturierter Form im sogenannten Package-Format übergeben.

Request und Response beginnen mit einem eindeutigen Command-Identifier. Danach werden die Inhalte der Felder mit definierten, festen Längen in vorgegebener Reihenfolge übergeben. Zum Schluss werden Felder mit variabler Länge und definierten Feldindikatoren übergeben.

Auf Grund der linearen Struktur lassen sich multiple Angaben nicht abbilden.

Definierte Vorgaben für die Belegung sind nur an wenigen Stellen vorhanden. Damit ergeben sich vielfältige Möglichkeiten der Belegung. Kommandos müssen deshalb herstellerabhängig ausgewertet und beantwortet werden.

NCIP

Request und Response werden im XML-Format (Extensible Markup Language) übergeben. Damit existieren jeweils genaue Beschreibungsmöglichkeiten in Form einer DTD (Document Type Definition). Request und Response können mit sogenannten Parsern jeweils überprüft werden. Für den strukturellen Aufbau existiert ein eindeutiges XML-Regelwerk.

Hierarchische Strukturen, die für multiple Angaben so wichtig sind, lassen sich hierbei genau abbilden. Hat ein Benutzer zum Beispiel verschiedene Sperren, die eine Ausleihe nicht zulassen, so können hier alle Gründe detailliert bekanntgegeben werden. Auch unterschiedliche Gebühren können nur unter Verwendung hierarchischer Strukturen genau abgebildet werden.

NCIP verwendet spezifizierte Datentypen (Enumerated Data Types). Erweiterungen müssen in Profilen bekannt gegeben werden. Muss das LMS zum Beispiel eine Aktion (Ausleihe, Rückgabe oder Verlängerung) ablehnen, so gibt es pro Request eine Menge von zulässigen Fehlermeldungen. Für diese sind keinerlei individuelle Absprachen und Umsetzungen notwendig. Die Aufgabe des Selbstbedienungsautomaten besteht dann darin, diese Meldungen in die gewünschte Sprache bibliotheksspezifisch umzusetzen.

Signifikante Unterschiede

Ausgabe komplexer Informationen

Mit SIP2 können komplexe Angaben in individueller Form übergeben werden. Die Angaben für die Sortierung, die Bildschirmausgabe oder die Ausgabe auf einem Quittungsdrucker können beliebig mit »sort bin«, »screen message« bzw. »print line« übergeben werden. Das ist für die Realisierung in einer Bibliothek sehr bequem, jedoch müssen diese für jede Bibliothek individuell angepasst werden. Mit NCIP müssen diese Angaben detailliert und typgerecht angegeben werden.

So ergibt sich aus dem NCIP-Protokoll eine strikte Trennung der Aufgaben zwischen Automat und LMS. Das LMS übergibt strukturierte, definierte Daten und der Automat bildet daraus die entsprechenden Ausgaben für Bildschirm und Drucker. Diese Trennschärfe ist bei Verwendung von SIP2 so nicht erkennbar.

Für die Definition einer Sortieranlage ist es zudem günstiger, aus mehreren, strukturierten NCIP-Angaben eines Exemplars die richtige Sortierbox jeweils im entsprechenden Rückgabeautomaten zu ermitteln. Da in einem Bibliothekssystem mit unterschiedlichen Standorten auch unterschiedliche Rückgabeautomaten mit abweichenden Sortierboxen vorhanden sein können und sich diese Sortiervorgaben auch ändern können, sollten diese Sortiereinstellungen am Rückgabeautomaten vorgenommen werden können. Günstig sind dabei Einstellungen, die keine Programmänderung erfordern und die die jeweilige Bibliothek selbst vornehmen kann.

Authentifizierung

Mit NCIP kann im Request genau angegeben werden, wie die Authentifizierung erfolgen soll. Genaue Angaben, ob die Anmeldung mit oder ohne Passwort und mit Ausweisnummer oder einer anderen Nummer erfolgen soll, sind hier möglich. Diese Einstellungen fehlen bei SIP2. Hier können nur »patron identifier« und »password identifier« angegeben werden. Die Definition, was der »patron identifier« ist, unterliegt der genaueren Absprache zwischen den Herstellern der Automaten und des LMS.

Kennzeichnung eines Exemplars

Auch hier kann im NCIP-Request genau angeben werden, mit welchen Angaben das Exemplar ermittelt werden soll. Das kann die eindeutige Mediennummer aber auch die UID des RFID-Chips sein. Im SIP2-Request ist hierzu keine spezifizierte Angabe möglich.

Anzeige eines Exemplars

Strukturierte Titelinformationen wie Titel, Autoren, Verlag, Erscheinungsjahr usw. lassen sich nur mit NCIP erzeugen. In SIP2 gibt es mit »title identifier« keine definierte Ausgabe.

Anzeige Benutzerkonto

Mit NCIP können Ausleihen oder Bestellungen einzeln mit vielen Angaben strukturiert und mit fest definierten Werten ausgegeben werden. Bei SIP2 ist die Ausgabe unstrukturiert und damit individuell gestaltet.

Strukturierte Angaben von Gebühren, Sperren und Adressangaben sind nur mit NCIP möglich.

Alle Exemplare verlängern

Bei NCIP gibt es keine Möglichkeit, alle ausgeliehenen Exemplare eines Benutzers mit einem Request zu verlängern. Jedes Exemplar muss einzeln mit einem Request verlängert werden. In SIP2 steht für die Gesamtverlängerung der Request »renew all« zur Verfügung.

Vorgang Ausleihe oder Rückgabe widerrufen

Wenn ein Ausleihvorgang wieder rückgängig gemacht werden soll, weil der Benutzer z. B. das Exemplar zu schnell vom RFID-Reader entfernt hat und der Schreibvorgang für das AFI-Flag für die Sicherung der Medien nicht erfolgen konnte, kann das mit dem NCIP-Request »UndoCheckout« erfolgen. Für die Rückgabe steht ein solcher Request nicht zur Verfügung. Man geht davon aus, dass im Rückgabeautomaten ein Exemplar kaum vom Benutzer wieder »herausgeholt« werden kann. Mit SIP2 gibt es dagegen »cancel« sowohl für die Ausleihe als auch die Rückgabe.

Fazit

Sowohl SIP2 als auch NCIP sind für die Gestaltung der Schnittstelle zwischen Selbstverbuchungsautomat und LMS geeignet. Mit SIP2 lassen sich jedoch nur Lösungen erzielen, die mit individuellen Absprachen zwischen den Herstellern der Software für die Automaten und des LMS einhergehen. Das kann für beide Partner mit einem hohen Zeitaufwand verbunden sein. Dabei kann sich der Kostenaufwand für die Hersteller und damit auch für die Bibliothek erheblich erhöhen. Nach dem nun für die RFID-Tags selbst ein Standard (dänisches Datenmodell für Bibliotheken) entwickelt wurde, wäre es wünschenswert, die Standardisierung der Schnittstelle zwischen Automaten und LMS

voranzutreiben. Unsere Erfahrungen als Entwickler von Bibliothekssoftware zeigen, dass die Verwendung des NCIP-Protokolls bei Implementationen für verschiedenste Bibliotheken die Arbeit wesentlich erleichtert hat.

Auch über die reine Selbstverbuchung hinaus ist dieses Protokoll bestens geeignet, selbst komplizierte Bezahlfunktionen am Kassenautomaten zu bedienen. Eine weitere Möglichkeit besteht in der Anfrage fremder Bibliotheken nach bestellbaren, verfügbaren Exemplaren zu einem gewünschten Titel. Dieses kann in Verbundsystemen als Vorstufe für die Fernleihe genutzt werden.

Für ein integriertes Bibliothekssystem betrachten wir es als selbstverständlich, die RFID-Technologie auch in die Arbeitsabläufe im Bibliotheksystem selbst zu integrieren. Das betrifft die Vorgänge Konvertieren, Löschen sowie alle weiteren Bearbeitungsfunktionen von Exemplaren.

Literatur und Internetquellen

[1] 3M ™ Standard Interchange Protocol, http://solutions.3m.com/wps/portal/3M/en_US/library/home/resources/protocols/

[2] ANSI/NISO Z39.83-1 und ANSI/NISO Z39.83-2, http://www.niso.org./kst/reports/standards

[3] Barbara Michaelis (2009): Vergleich der Schnittstellen SPI2 und NCIP (PDF), http://www.th-wildau.de/hochschule/einrichtungen/bibliothek/die-bibliothek-vor-ort/veranstaltungen-events/2-wildauer-symposium-rfid-und-medien.html

Die zitierten Internetquellen wurden zuletzt am 14.05.2010 aufgerufen.

Die Datenmodellstandardisierung und ihre Auswirkungen auf RFID-Bibliotheken

Christian Kern

Ausgangslage

Bereits 2002, als sich die ersten Bibliotheken für den Einsatz von RFID-Systemen entschlossen, wurde auf vorhandene Standards für die Entwicklung der Selbstverbuchung und Mediensicherung zurückgegriffen. Ohne diese wäre der heutige Markt für RFID-Systeme in Bibliotheken nicht entstanden. Dabei handelte es sich, erstens, um das SIP2-Protokoll (Standard Interchange Protocol 2[1]) für die Verbindung zwischen RFID-System und Bibliotheks-Management-System (LMS, Library Management System). Zweitens war der RFID-Standard ISO 15693[2] ausschlaggebend, welcher die so genannte Luftschnittstelle zwischen RFID-Etiketten und Lesegeräten beschrieb und aus dem Smartcard-Bereich stammte. Dieser Standard war die wichtigste technische Voraussetzung für die Entwicklung des Massenmarktes für RFID-Etiketten. Weitere Standards und Regelwerke existierten zur Sendeleistung und CE-Zeichen, und schliesslich gab es noch die so genannte ISIL-Nummer (International Standard Identifier for Libraries). Als eindeutige Bibliothekskennzeichnung wird sie für die Zuordnung der Medien zu einer spezifischen Bibliothek genutzt. Die jeweiligen Mediennummern einer Bibliothek zusammen mit der ISIL ermöglichen weltweit eine eindeutige Kennzeichnung der Medien.

Die jüngste Entwicklung in diesem Reigen der Standards – und dies ist auch ein Novum innerhalb anderer RFID-Anwendungen (Logistik, Lagerhaltung, Prozesskontrolle usw.) – ist die Festlegung eines Datenmodells für die RFID-Etiketten in ISO 28560, d. h. ihres Dateninhaltes und dessen Schreibweise im Speicher[3] eines RFID-Chips. Neu ist daran, dass nicht nur die Art der Kommunikation (im übertragenen Sinne auf die Sprache: wie werden Buchstaben ausgetauscht), sondern auch deren Inhalt (Festlegung der Sprache, Wörter und Inhalte) definiert werden. Im Folgenden werden der heutige Status, die bereits sichtbaren und zukünftigen Auswirkungen der Datenmodellstandardisierung beschrieben.

Was ist ein RFID-Datenmodell für Bibliotheken und wie wirkt es sich aus?

Ein Beispiel verdeutlicht die Konsequenzen fehlender Standards: Im Jahre 2002 wurden in der Rockefeller Library in New York proprietäre Chips eines bestimmten Lieferanten verwendet. Nach einiger Zeit konnten keine Etiketten mehr nachgeliefert werden, weil der Chipproduzent keine kompatiblen Halbleiter der ersten Generation mehr herstellte.

1 Entwickelt von 3M. Später ergänzt durch ein Protokoll der NISO (National Information Standards Organization)

2 Später in ISO 18000-3.1 integriert

3 RFID-Chips sind einfache, über Funk ansprechbare Datenträger (sie enthalten ein EEPROM). Die Daten können auf Speicherseiten abgelegt werden.

Folglich mussten die bestehenden RFID-Etiketten aus den Büchern herausgetrennt und durch neue ersetzt werden. Dies bedeutete bei 100‘000 Medien nicht nur einen grossen Arbeitsaufwand, sondern führte auch zur Beschädigung der Medien durch das Entfernen der veralteten Etiketten. Dieser Vorfall fand nur wenig Beachtung in den Fachzeitschriften, da dieses Problem als Einzelfall betrachtet wurde. Nach diesem »worst case« wurden jedoch in allen folgenden Installationen in den USA und Europa Chips nach ISO 15693 (heute ISO 18000-3.1) eingesetzt. Dadurch konnte auf der Chipebene eine langfristige Versorgung der Bibliotheken sichergestellt werden. Nun war es zumindest theoretisch möglich, die Chips verschiedener Hersteller, die alle diesem Standard unterlagen, innerhalb einer Bibliothek einzusetzen.

Die Standardisierung eines Datenmodells wirkt sich auf einer weiteren Ebene aus. Sie führt nicht nur zu einer Austauschbarkeit der Chips, sondern sämtlicher RFID-Geräte, wie Sicherungsgates, Verbuchungsstationen usw...

Doch betrachten wir zunächst die Ausgangslage. RFID-Bibliotheken nutzen heute, weltweit, mehrheitlich proprietäre, d. h. nicht standardisierte Datenmodelle. Damit ist ein sicherer Betrieb der Bibliothek durchaus gewährleistet – solange der Lieferant nicht gewechselt wird.

Ein proprietäres Datenmodell bedeutet, dass der Lieferant die Daten so in die Etiketten schreibt, dass diese nur von ihm selbst entschlüsselt werden können. Im übertragenen Sinne spricht also jeder Lieferant seine eigene Sprache. Dadurch kann er, falls erforderlich, der Bibliothek zwar verschiedene Chipversionen vom gleichen Standard anbieten, aber sie kann den Lieferanten nicht wechseln. Der Lieferant verwendet sein proprietäres Datenmodell folglich als Kundenbindungsmassnahme. Bei einem Systemwechsel müssten also sämtliche Etiketten neu beschrieben (nicht ausgetauscht) werden. Da der neue Lieferant die RFID-Chips aber nicht lesen kann, können diese nicht einfach beim Verbuchungsvorgang gelesen und umgeschrieben werden. Sie müssen vielmehr neu initialisiert, d. h. bei jedem Medium der Barcode neu eingelesen werden.

Stellung der Bibliotheken innerhalb der weiteren RFID-Anwendungen

Mit dem zunehmenden Einsatz von RFID-Systemen hat sich auch die Bedeutung der Bibliotheken innerhalb der RFID-Industrie verändert. Sie sind zu einem Kundensegment geworden, das nachhaltig attraktive Stückzahlen an RFID-Etiketten und Lesegeräten abnimmt. So weckt der Bibliotheksmarkt die Aufmerksamkeit verschiedenster Lieferanten. Dies ist durchaus im Interesse der Bibliotheken. Durch die Konkurrenzsituation bleibt der Markt in Bewegung, Preise sinken und die Versorgung ist sichergestellt.

Die Notwendigkeit der Datenmodellstandardisierung wird auch durch den hohen Anspruch der Bibliotheken an die Lebensdauer der Etiketten gestellt. Bibliotheken »leben« grundsätzlich länger als viele Firmen, denn es sind öffentliche Einrichtungen. Sie müssen also zwingend damit rechnen, dass Etiketten irgend wann nicht mehr funktionieren und/oder Lieferanten im Laufe der Jahre vom Markt verschwinden. Die

Datenmodellstandardisierung ist also sowohl ein Kosten- wie auch Versorgungsthema, mit mittel- bis langfristigen Auswirkungen.

Bisher stand in der Diskussion über einen Datenmodellstandard so genannte Interlibrary Loan (ILL) im Vordergrund. Er ermöglicht den Austausch von Medien zwischen den Bibliotheken, für den ein standardisiertes Datenmodel die Basis ist. Bei näherer Betrachtung sieht man allerdings, dass der ILL von untergeordneter Bedeutung ist. Der Austausch von Medien bleibt so lange mit traditionellen Mitteln (mit Zetteln und Belegen) durchführbar, wie die Mengen der ausgetauschten Medien auf heutigem überschaubarem Niveau bleiben. Ausserdem wird das gelieferte Buch im ILL nicht in den Medienkreislauf der ausleihenden Bibliothek integriert, sondern stets extra behandelt. Einzig bei der Rückgabe an RFID-Automaten könnten Komplikationen auftreten, wenn ein nicht zur Bibliothek gehörendes Medium mit einem unbekannten Datenmodell angenommen werden müsste. Gegenüber dem ILL ist die Austauschbarkeit der RFID-Komponenten in der Bibliothek, d. h. die Möglichkeit zum Wechsel des Lieferanten, von viel grösserer Bedeutung.

Entwicklung der Standardisierungsarbeiten

Der erste Ansatz für ein standardisiertes Datenmodell kam 2005 aus den Niederlanden. Dort werden die Nummernkreise für die Medien der nationalen Bibliotheken zentral von der NBD Biblion (Verband der Niederländischen öffentlichen Bibliotheken) vergeben und verwaltet. Dieses Recht wurde auf RFID-Etiketten ausgeweitet und ein eigenes Datenmodell geschaffen. Dieses wurde offen gelegt, aber die NBD behielt die Rechte an den Daten. Sämtliche RFID-Etiketten wurden zentral eingekauft und vorprogrammiert.

Der zentrale Einkauf von RFID-Etiketten wurde nach einiger Zeit aufgegeben. Der Druck, aufgrund der ausländischen Anbieter ständig die Preise anzupassen, wurde so gross, dass sich der Etikettenvertrieb schliesslich nicht mehr lohnte. Heute besteht nur noch der Eigentumsanspruch auf die Mediennummern. Keine Organisation hat dies in ähnlicher Weise durchgesetzt. Umso bemerkenswerter war dieser Sonderweg, da die Niederlande an der Datenmodellstandardisierung in der ISO intensiv mitarbeiteten.

Kurz nach dem Start des NBD-Modells in den Niederlanden wurde das Thema in Dänemark, Deutschland, der Schweiz und Österreich aufgegriffen. In Kopenhagen, am Institut des Dansk Standard (DS) trafen sich erstmals Repräsentanten fast aller RFID-Systemlieferanten an einem runden Tisch, um die technischen Parameter festzulegen, d. h. zu entscheiden welche Daten sinnvoll aufzunehmen und wie diese konkret auf die Chips zu schreiben wären. Im deutschsprachigen Arbeitskreis MSHW (Vertreter der Bibliotheken aus München, Stuttgart, Hamburg, Luzern, Wien) wurden die bibliothekarischen Anforderungen geprüft (welche Daten sinnvoll in den Chip geschrieben werden sollten). Zusätzlich wurde ein AFI-Wert für die Sicherung der Medien bei der ISO beantragt[4].

4 Die Klärung und Beantragung des AFI-Wertes (Application Family Identifier) war ein wichtiger Meilenstein. Sie besaß eine ähnliche Bedeutung wie das Datenmodell für die Kompatibilität der RFID-Systeme in Bibliotheken.

Das Ergebnis war ein dem NBD-Modell ähnliches, aber freies Datenmodell, weil es keine Rechte an Mediennummern festschrieb. Dieses Resultat ist heute als »Dänisches Datenmodell« bekannt. Es wird heute in fast allen Ausschreibungen für RFID-Bibliothekssysteme in Zentral- und Nordeuropa vorgeschrieben. In diversen weiteren Ländern wurden daraufhin Derivate des dänischen Modells entwickelt, die jedoch im Zuge der internationalen Standardisierung auf ISO-Ebene wieder aufgegeben werden. Das Dänische Datenmodell ist als Teil (-3) in ISO 28560 enthalten.

Auch ohne die Festschreibung auf ISO-Ebene hätte sich das Dänische Modell als ein Defacto-Standard durchgesetzt. Es hat in den zurückliegenden Jahren seine Eignung in der Praxis bewiesen. Es sind von den Bibliotheken, welche es bis heute einsetzen, keine Anpassungen oder Erweiterungen gewünscht worden.

Inhaltliche Fragen

ISO 28560-3 ist inhaltlich in zwei Hauptabschnitte unterteilt:
- Der **Mandatory Part** enthält die unbedingt erforderlichen Daten, wie z. B. die Mediennummer, Medienpakete und ISIL-Nummer. Er hat einen Mindestumfang von 256 bit.
- Der **Optional Part** hat eine fast beliebige Grösse und Inhalt. Es nutzt den Speicher über 256 bit hinaus (übliche RFID-Chips haben einen Speicher von 1 bis 2 kbit). In diesem Teil können zum Beispiel Verlage oder Lieferanten logistische Daten hinterlegen. Diese können durchaus verschlüsselt sein.

2007 trat in Kopenhagen die Arbeitsgruppe mit der Bezeichnung ISO-TC46 SC4 WG11 zusammen. Vertreter aus Australien, Dänemark, Deutschland, Finnland, Frankreich, Italien, Neuseeland, Niederlande, Japan, Schweden, Schweiz, Südafrika, Vereinigtes Königreich und den USA beteiligten sich.

Entgegen den ursprünglichen Erwartungen wurde zuerst nicht das bisherige Dänische Datenmodell 1:1 übernommen, sondern versucht, ein vollkommen Neues Modell vorzuschlagen. Es basierte auf einem im Bereich Fluggepäck diskutierten Modell (ISO 15962), welches ein hohes Mass an Flexibilität ermöglichte, da die Felder des Chip-Speichers variabel beschrieben werden konnten. Dieser neue Ansatz kam vielen ISO-Mitgliedern entgegen, da in einigen Ländern noch Uneinigkeit über die eigentlichen Dateninhalte auf dem Chip herrschte. So betrachteten manche Vertreter es als wichtig, dass auch der Buchtitel mit auf dem Chip gespeichert würde. Andere hingegen waren der Meinung, dass diese Inhalte jederzeit vom LMS aus bezogen werden könnten und eine einfache Nummer als Bezug zu den Inhalten ausreichend wäre.

Der neue Vorschlag deckte alle Eventualitäten ab. Es wurden OIDs, so genannte Object Identifier, eingesetzt. Sie verweisen über eine Nummer auf den Speicherbereich im Chip mit der jeweiligen Information. Dieses Modell kann an verschiedene Chipgrössen angepasst werden. Eine wichtige Überlegung für dieses OID-Datenmodell war, dass die Verlage die RFID-Etiketten mit ihren Daten integrieren und diese anschliessend in der Logistikkette, bis in die Bibliothek hinein nutzen können.

Aufgrund des Einspruches mehrerer Mitglieder wurde jedoch das bisher erarbeitete und bereits in mehreren Ländern etablierte Dänische Datenmodell als eigener Teil 3 mit aufgenommen.

ISO 28560 enthält heute drei Teile mit folgendem Inhalt:

ISO 28560-1 enthält eine Beschreibung vielfältiger, für Bibliotheken denkbarer Datenelemente. Dies sind neben der Mediennummer auch den Titel von Büchern und weitere Daten, welche eventuell offline verfügbar auf dem Chip sein sollten. Aus den Elementen kann für jedes Land ein »Profil« zusammengestellt werden.

ISO 28560 Teil 2 basiert wiederum auf ISO 15962 und den oben genannten OIDs. Er wird in den angelsächsischen Ländern stark propagiert. In diesen Ländern sind bisher vorwiegend proprietäre Datenmodelle im Einsatz, das Dänische Modell kaum verbreitet.

ISO 28560 Teil 3 entspricht zu fast hundert Prozent dem Dänischen Datenmodell. Es ist im Vergleich zum Teil 2 zwar fest kodiert, aber deutlich einfacher strukturiert.

Fazit

Das Dänische Datenmodell findet sich im Teil 3 von ISO 28560 wieder. Teil 3 wird vorrangig in den zentraleuropäischen und skandinavischen, weniger in den angelsächsischen Ländern eingesetzt. Für die Bibliotheken ist aber mit beiden Teilen, 2 und 3, vorerst eine gute Grundlage geschaffen, auf die sie sich in Ausschreibungen beziehen können. Momentan ist es nicht so wichtig, *welcher* Standard sich durchsetzt, sondern *dass* überhaupt ein solcher verwendet wird.

Die Folgen der Standardisierung sind heute erkennbar. Es ist durch die Unabhängigkeit der Bibliotheken von den Lieferanten ein rapider Preisrückgang für die RFID-Etiketten eingetreten. Viele Bibliotheken konnten sich zu einem früheren Zeitpunkt ein RFID-System leisten. Eine weitere Folge ist, dass die Marktentwicklung viel schneller voranschritt, als dies ursprünglich von den Systemanbietern erwartet wurde. Eine erhöhte Transparenz und abnehmende Preise halten sie in Atem. In den angelsächsischen Ländern wird, im Vergleich zu den zentraleuropäischen, der Markt von sehr wenigen Systemlieferanten bestimmt. Dementsprechend ist das Preisniveau dort höher. Dies hat eine Studie 2010 herausgestellt (Mick Fortune[5]).

Aus heutiger Sicht macht ein gemeinsamer, zentraler Einkauf von RFID-Etiketten durch Verbände oder gar Verlage, nur wenig Sinn, weil neue Abhängigkeiten entstehen. Die Bibliotheken sind gut beraten, auch weiterhin den Markt scharf zu beobachten.

5 http://www.mickfortune.com/Wordpress/?page_id=201

Qualitätsmerkmale von RFID Etiketten

Josef Bernhard, Tobias Dräger

Um die Qualität eines RFID Etiketts objektiv und reproduzierbar bewerten zu können sind entsprechende Qualitätsmerkmale und Prüfverfahren notwendig. In diesem Beitrag wird kurz auf Qualitätsmerkmale im Bezug auf RFID Etiketten eingegangen und die aktuelle Situation bei der Definition von Testkriterien und- verfahren dargestellt.

Motivation

Für die Performance eines RFID Systems ist nicht nur der RFID Leser oder Reader wichtig, sondern auch die Qualität der RFID Etiketten oder Transponder entscheidend. Da die RFID Transponder, die an den Medien angebracht werden, in großen Mengen verwendet werden, ist der Preis des RFID Etiketts ein wichtiger Faktor. Getrieben durch Anwendungen im Bereich der Konsumgüterindustrie sind die Preise für RFID Etiketten insbesondere der UHF-Technologie, aber auch der HF-Technologie in den letzten Jahren massiv gesunken. Damit sich dieser Preisverfall nicht auf die Qualität niederschlägt, ist es wichtig, die Qualität der Labels von Zeit zu Zeit zu überprüfen und objektiv zu bewerten. Dieser Beitrag widmet sich dem Thema Qualitätsmerkmale bei RFID Transpondern, insbesondere der RFID Etiketten im Frequenzbereich 13,56 MHz, die derzeit fast ausschließlich in Bibliotheken zum Einsatz kommen. Es soll ein Überblick gegeben werden, welche Merkmale zur Beurteilung eines RFID Transponders herangezogen werden können und welche Normen bereits existieren.

Merkmale zur Qualitätsbeurteilung

Elektrische Eigenschaften

Als elektrische Eigenschaften werden hier die auf die Luftschnittstelle bezogenen Kennwerte eines RFID Systems verstanden. Für den Anwender ist das im Wesentlichen die Lesereichweite, die mit einem bestimmten RFID System, bestehend aus einem RFID Reader und einem RFID Transponder, erreicht werden kann. Hat der Anwender eine bestimmte Infrastruktur, sprich RFID Reader installiert, möchte er möglichst mit Etiketten unterschiedlicher Hersteller eine gleich gute Reichweite erzielen. Die Labelhersteller wiederum werden versuchen, eine möglichst gleich gute Qualität bei unterschiedlichen Readern zu erzielen. Für eine zuverlässige Funktion in der Praxis wird beispielsweise eine Lesereichweite am Selbstverbucher von etwa 35 cm erwartet, wenn der RFID Transponder am Medium angebracht ist. Die Lesereichweite eines Transponders an einem bestimmten, verbauten Leser zu bestimmen ist zwar keine objektiv ausreichende Messung, liefert aber für den Anwender in der Praxis eine gute Basis. Aus wissenschaftlicher Sicht

ist diese Methode allerdings fehlerbehaftet, weil die Testumgebung nicht spezifiziert ist und damit die Messung insbesondere durch Einflüsse:
- unterschiedlicher Reader
- der Umgebung des Readers
- des Mediums
- unterschiedlicher Positionierung der Medien

verfälscht wird.

Die Reproduzierbarkeit der einzelnen Messungen und der Vergleichbarkeit der Messungen untereinander ist dadurch schwierig. Für eine objektive Charakterisierung muss also die Messumgebung klar definiert sein.

Andere relevante elektrische Leistungseigenschaften sind die Datenerhaltungszeit der gespeicherten Daten auf dem Chip und die Pulkerfassungsmöglichkeiten, also die gleichzeitige Erfassung von mehreren Transpondern.

Mechanische Eigenschaften

Zu den mechanischen Eigenschaften zählen Eigenschaften wie:
- Festigkeit und Langlebigkeit der Klebeverbindung
- Beständigkeit der Labeloberfläche
- Beständigkeit der Aufbau- und Verbindungstechnik des Etiketts (z. B. Antenne-Chip Verbindung)

Insbesondere für die mechanischen Eigenschaften sind Alterungstests zu definieren, aus denen zuverlässige Aussagen über die langfristige Beständigkeit der mechanischen Festigkeit des Labels abgeleitet werden können. Die mechanischen Eigenschaften zusammen mit der Erhaltungszeit der Daten auf dem Speicher des Mikrochips bestimmen die Nutzungsdauer des RFID Etiketts. Dabei ist die Gesamtlebensdauer nur so gut wie das schwächste Glied in der Kette.

Zur Funktion des RFID Systems

Zur Charakterisierung der RFID Technologie, insbesondere einzelner Komponenten eines RFID Systems, ist eine kurze Beschreibung der Technologie erforderlich, die sich im Folgenden auf die HF-Technologie bei 13,56 MHz beschränken soll.

Ein RFID System bei 13,56 MHz kann als einfacher Transformator beschrieben werden, bei dem eine Primärspule, in diesem Fall des Readers, mit einer Sekundärspule im Transponder über das magnetische Feld verkoppelt ist.

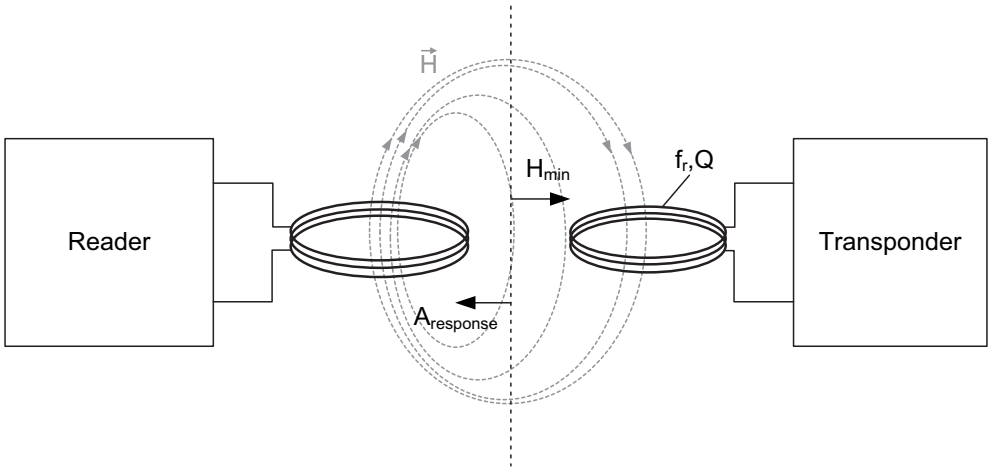


Abb. 1: RFID System mit gekoppelten Spulen

Über dieses verkoppelte Spulensystem wird einerseits Energie vom Reader an den Transponder übertragen und anderseits Information zwischen den beiden Komponenten ausgetauscht. Die Sekundärspule ist mit der Transponderelektronik verbunden, ein elektronischer Schaltkreis, der mit Energie versorgt werden muss. Da eine Batterie oder Akku für die meisten RFID Anwendungen zu teuer wäre, muss die Energie über das Feld der verkoppelten Spulen von der Primärseite – also dem Reader – zur Sekundärseite übertragen werden. Je besser die Spulen miteinander verkoppelt sind, desto mehr Energie kann übertragen werden.

Ein Maß für die Verkopplung der beiden Spulen ist der Koppelfaktor k. Es gibt verschiedene Faktoren, die den Koppelfaktor zwischen Reader- und Transponderspule beeinflussen:

- Die Geometrie, Windungszahl und Größen der Spulen
- Die Distanz zwischen Primär- und Sekundärspule
- Die Umgebung der Spulenantennen

Der Graph in der Abbildung zeigt qualitativ, wie stark der Koppelfaktor über den Abstand abfällt. Der Abstand ist in der Grafik normiert auf den Spulenradius r1 der Primärspule.

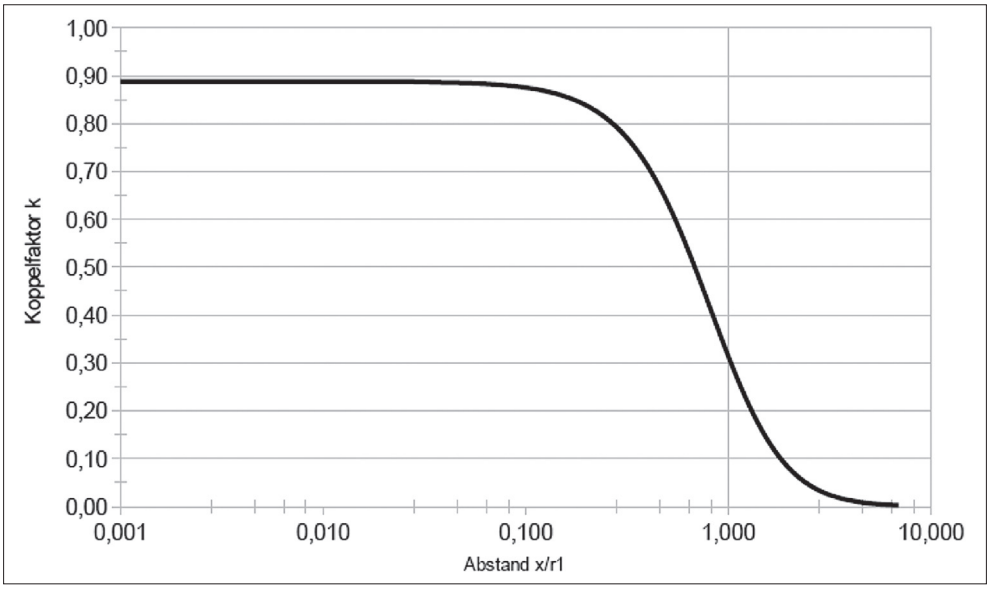


Abb. 2: Verlauf Koppelfaktor, auf Spulenradius normiert

Für die Energieausbeute durch den elektronischen Schaltkreis auf der Sekundärseite ist überdies entscheidend, wie der Chip an die Spule kontaktiert ist. Dies ist auch ein entscheidendes Merkmal für die Qualität der Datenübertragung zwischen Reader und Transponder und umgekehrt. Die Transponderspulen werden auf Resonanz abgestimmt, um eine höhere Energieausbeute zu erzielen. Die Resonanzfrequenz kann durch die Umgebung verstimmt werden, insbesondere durch das Aufbringen der Etiketten auf Medien wie Bücher und CDs. Die Verstimmung der Resonanzfrequenz durch die Umgebung kann, sofern sie bekannt und einigermaßen konstant ist, bei der Herstellung der Transponder berücksichtigt werden. Ein solcher angepasster Transponder hat dann erst bei Anbringung auf das Medium seine optimale Performance. Durch die sehr unterschiedlichen Medien, die in der Praxis zum Einsatz kommen, ist es nicht möglich die Resonanzfrequenz eines RFID Transponder so abzustimmen, dass sie für alle Medien exakt gleich ist. Es ist ein Kompromiss zu wählen, der innerhalb eines definierten Toleranzbandes liegt.

Charakterisierung von RFID Transponder

Wie beschrieben handelt es sich bei einem RFID System im 13,56 MHz Bereich um ein verkoppeltes System. Deshalb ist es außerordentlich schwierig, die Performance eines Transponders für sich zu bestimmen, da er immer in Wechselwirkung mit dem Reader steht. Je nach Reader, Readerantenne und Umgebung können mit einem RFID Transponder unterschiedliche Reichweiten erzielt werden. Ebenso kann ein Reader mit Transpondern verschiedener Hersteller unterschiedlich gut zusammenarbeiten. Deshalb wird der Transponder in einem genau definierten Readerumfeld charakterisiert.

Zur Charakterisierung wird nicht die Reichweite herangezogen, sondern spezifische Merkmale der Luftschnittstelle. Dies ist zum einen die *Ansprechfeldstärke* H_{min} des Transponders, also die Feldstärke, die minimal vom Reader erzeugt werden muss, um den Transponder zu aktivieren, ihn also mit ausreichend Energie zu versorgen. Zum anderen wird die *Amplitude des Antwortsignals* $A_{Response}$, das vom Transponder erzeugt wird an der Empfangsspule des Readers gemessen. Aus diesen beiden Kennwerten eines Transponders lässt sich dann die mit einem gegebenen Reader erzielbare Reichweite berechnen. Es gibt zwei Reichweitenbegrenzungen im System:

1. Bis zu welcher Distanz kann ein Reader die notwendige minimale Ansprechfeldstärke für einen Transponder erzeugen.
2. Aus welcher Distanz ist der Reader noch in der Lage das vom Transponder erzeugte Antwortsignal zu detektieren.

Man überprüft also, ob ein Reader die benötigte Feldstärke bei der gewünschten Reichweite erzeugt und ob die Amplitudenänderungen, die die Transponderantworten am Ausgang der Primärantenne des Readers verursachen auch vom Reader detektiert werden können.

Zur Bestimmung dieser Parameter ist eine definierte Testumgebung notwendig. In internationalen Standards sind solche Setups festgelegt. So sind im Standard ISO10373 Testaufbauten und -methoden für die Charakterisierung von Chipkarten bei 13,56 MHz definiert. Andere RFID Transponderarten werden in ISO18046 und ISO18047 berücksichtigt. Diese Standards definieren auch zu prüfenden Merkmale und deren Grenzwerte. Bisher nicht definiert ist, wie der Einfluss unterschiedlicher Medien berücksichtigt werden kann. Da die Variation der Medien in Größe, Dicke und Beschaffenheit des Materials wie etwa des Einbandes eines Buches sehr groß ist, muss versucht werden einige wenige Referenzmedien festzulegen, die einen Großteil der Medien am Besten repräsentiert. Ausnahmemedien, die nicht vom Referenzmedium abgedeckt werden, wird es aber immer geben.

Um das Verhalten der Transponder noch genauer zu ermitteln, können die Parameter über einen größeren Frequenzbereich gemessen werden. Durch diese Messung erhält man eine Aussage über die Resonanzfrequenz der RFID Transponderantenne. Idealerweise sollte die Resonanzfrequenz des Transponders bei 13,56 MHz liegen, um eine möglichst hohe Reichweite zu erzielen. In der Praxis kann sich aber durch die Umgebung die Resonanzfrequenz verschieben. Dies geschieht insbesondere durch das Medium selber, auf dem das RFID Etikett angebracht wird. Auch die Transponder selber können sich gegenseitig beeinflussen, wenn sie zu nahe aneinander gebracht werden.

Weiterhin spielt die Güte der Spule eine entscheidende Rolle. Je höher die Güte, desto größer die empfangene Energie am Transponder. Mit einer höheren Güte wird aber auch die Bandbreite kleiner, was sich wiederum negativ auf die Amplitude des Antwortsignals des Transponders auswirkt. Die Güte einer Spule wird sowohl vom Aufbau der Spule als auch von der Umgebung also beispielsweise vom Medium beeinflusst.

Auswirkungen der Medien auf die Transponder

Die Medien haben Auswirkungen auf die RFID Etiketten, insbesondere wird die Resonanzfrequenz der Transponder durch die Beschaffenheit der Medien verstimmt. Abbildung 3 zeigt exemplarisch Messungen der Resonanzfrequenz verschiedener RFID Etiketten mit und ohne Medium. Es wurde dabei mit 4 verschiedenen Medien gemessen. Es ist deutlich zu erkennen, dass sich die Resonanzfrequenzen durch die Medien nach unten zur nominellen Resonanzfrequenz von 13,56 MHz hin verschieben.

Ohne Medium liegen die Resonanzfrequenzen meist über 13,56 MHz. Die Höhe der Frequenzverschiebung ist bei den verschiedenen Transpondertypen unterschiedlich. Wie das Diagramm ebenfalls zeigt variiert die Frequenzverschiebung auch mit der Art und Beschaffenheit des Mediums.

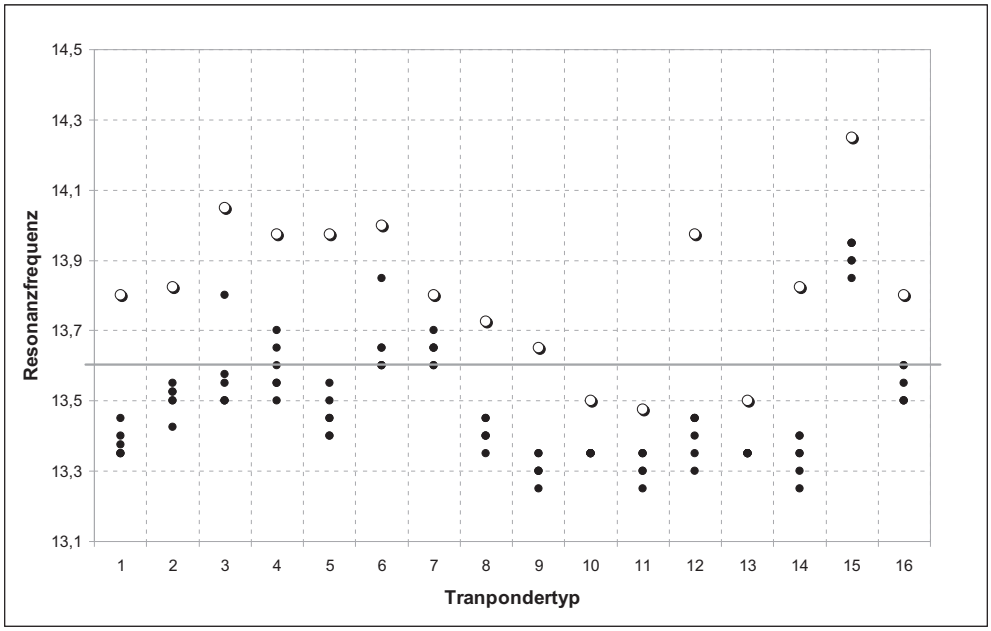


Abb. 3: Messung der Resonanzfrequenz verschiedener Transponder mit verschiedenen Medien (schwarz) und ohne Medium (weiss).

Durch die individuelle Ausgestaltung der RFID Etiketten durch den Hersteller können die Auswirkungen durch die Medien kompensiert werden. Dabei spielt die Größe, Material und Form der Antennenspule auf dem Etikett eine wesentliche Rolle. Es können unterschiedliche Materialen wie Kupfer oder Aluminium verwendet werden. Die Anzahl und der Abstand der Windungen der Spule, sowie die Dicke der Leiterbahnen haben wesentlichen Einfluss auf die Resonanzfrequenz und Güte der Spule. Weiterhin kommen unterschiedliche Chips von verschiedenen Halbleiterherstellern zum Einsatz, die auch unterschiedlich kontaktiert werden können. Dadurch ergibt sich eine Vielzahl von Freiheitsgraden, mit denen ein RFID Etikett individuell an die jeweiligen Anforderungen angepasst werden kann. Entscheidend ist, die Anforderungen der Bibliothek und damit

im Wesentlichen die Auswirkungen verschiedener Medien auf das RFID Etikett korrekt zu bestimmen. Nur so ist eine bessere Auswahl oder Optimierung der RFID Etiketten für diese Anwendung möglich.

Zusammenfassung und Ausblick

Dieser Beitrag versucht auf das Thema Qualitätsstandards bei RFID Etiketten für den Einsatz in Bibliotheken einzugehen. Qualifizierungsnormen für HF-RFID Transponder bei 13,56 MHz existieren, müssen aber für die Anwendung im Bibliotheksbereich angepasst werden. Verbindliche Grenzwerte für minimale Ansprechfeldstärke, Amplitude des Transponder-Antwortsignals und der daraus resultierenden Reichweite auf dem Medium müssen für die Anwendung bei Bibliotheken und auf Medien noch festgelegt werden. Der dafür ins Leben gerufene runde Tisch zur Sicherung der Qualität von RFID Etiketten im Bibliothekswesen arbeitet mit den Herstellern von RFID Etiketten und Chips an einem verbindlichen Regelwerk für die Ausschreibung von RFID Etiketten.

Literatur und Internetquellen

[1] Finkenzeller, Klaus (2002): RFID Handbuch, 3. Auflage. Hansen Verlag München Wien, ISBN 3-446-22071-2

[2] ISO/IEC 10373: Identification Cards – Test methods

[3] ISO/IEC 18046 (2007): Information technology – Automatic identification and data capture techniques – Radio frequency identification device performance test methods

[4] ISO/IEC TR 18047-3 (2008): Information technology –Radio frequency identification device conformance test methods – Part 3: Test methods for air interface communications at 13, 56 MHz

Qualitätsbestimmung von RFID-Komponenten auf der Basis von allgemein anerkannten Normen und Richtlinien – Vereinfachung von Ausschreibungen

Frank Gillert, Hardy Zissel

Der Einsatz von RFID Systemen in Bibliotheken wird längst nicht mehr nur in der Gruppe der sogenannten »Early Adopters« diskutiert, sondern ist auf der Tagesordnung, wenn es um die Modernisierung von Bibliotheken geht. Seit kurzem werden Richtlinienarbeiten zum Einsatz von RFID-Systemen auf den Weg gebracht. Ziel ist es, ausgehend von einer ausschreibungsrelevanten Leistungsmetrik auch praktikable Abnahme- und Testverfahren abzuleiten, die gemäß dem Stand der Technik branchenweite Anerkennung finden. Um dieses Ziel zu erreichen, ist es zum einen von Bedeutung, die Anwender eng einzubinden, zum anderen alle weltweit bedeutenden Herstellerunternehmen zu involvieren. Ebenso sollte die Erarbeitung ganzheitlich erfolgen, indem Methoden des Qualitätsmanagements berücksichtigt werden.

Nicht zuletzt müssen Beschreibungen des Stands der Technik formal seitens offizieller Standardisierungsinstitutionen möglichst international publizierbar sein. Es wird ein Stufenmodell vorgestellt, das eine sofort verwertbare, deutsch-englische VDI-Richtlinie enthält, die direkt zur Unterstützung von Ausschreibungen genutzt werden kann und darauf aufbauend über die geeigneten Wege in den Standardisierungsprozess ISO integriert werden kann.

Einführung

Die logistischen Abläufe innerhalb einer Bibliothek sind vielfältig, zeitaufwendig und im Sinne des Lean Managements existieren Prozessteile, die der »Verschwendung« zu zuordnen sind. Derartige Prozessteile sind insb. zu vermeiden, da sie von hochqualifizierten Bibliothekaren zu Ungunsten der eigentlichen Aufgaben im Rahmen des Wissensmanagements vorgenommen werden. Um den Anforderungen an eine moderne Bibliothekslandschaft gerecht zu werden, die sich durch freien Zugang durch den Nutzer zu den Medien zu allen Zeiten (24/7) sowie flexible Ausleihe und Rückgabeprozesse auszeichnet, halten mehr und mehr innovative Lösungen aus den Bereichen Informations- und Kommunikationstechnologien Einzug in die Infrastruktur der Bibliotheken. Schwerpunkte sind automatische Identifikation, mobile Datenerfassungsgeräte sowie Ortungs-, Lokalisierungs- und Visualisierungstechnologien. Im Folgenden wird die RFID Technologie im Hinblick auf Bibliotheksprozesse näher betrachtet.

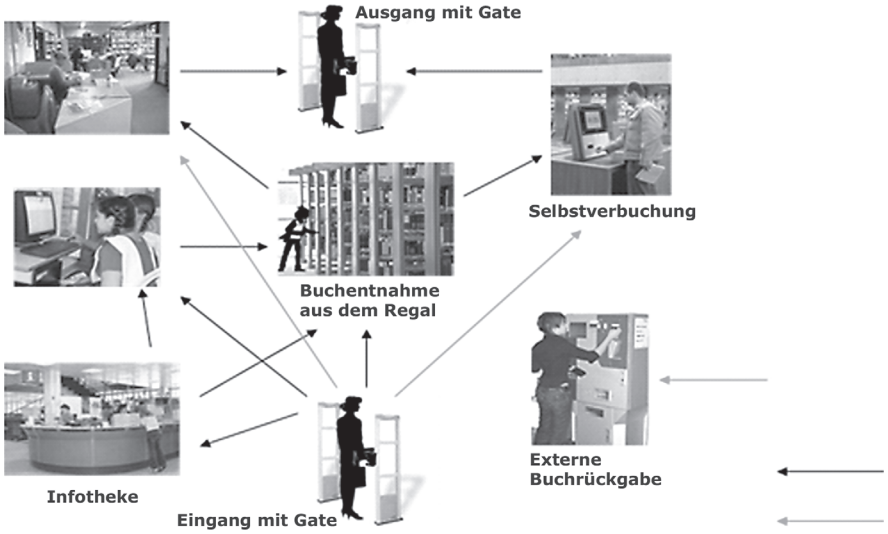


Abb. 1: Intralogistik-Abläufe in einer Bibliothek aus Sicht des Benutzers

Um diese Abläufe zu unterstützen, werden unterschiedliche RFID-Teilsysteme benötigt. Eine Einteilung von RFID-Systemen innerhalb von Bibliotheken lässt sich dabei folgendermaßen untergliedern:

- RFID Schleusensysteme
- RFID Selbstverbuchungsplätze
- RFID Rückgabeautomaten und Sortierstrecken
- RFID Personalarbeitsplätze
- RFID Handlesegeräte zur Inventarisierung
- RFID Konvertierungsplätze
- Transponder/Etiketten

Eine Unterscheidung der einzelnen Systeme ist wichtig, da je nach Einsatzort und Aufgabe andere Faktoren auf diese einwirken. Das können zum einen Umweltfaktoren sein, die sich unmittelbar aus der Umgebung herleiten lassen. Es können aber auch Einflussfaktoren sein, die sich aus der Benutzung des Gerätes erschließen. Um eine objektive Beurteilung der Leistungsfähigkeit zu erreichen, müssen daher die einzelnen Systeme getrennt betrachtet werden. Dies erfolgt im Rahmen dieses Konzeptes in der Analyse der funktionalen Parameter, getrennt für jedes Teilsystem.

Grundsätzlich kann gesagt werden, dass die Funktionsweise aller Teilsysteme ähnlich ist, da die Kommunikation über die Luftschnittstelle mit den Transpondern standardisiert erfolgt. Dabei besitzt jedes System ein Lesegerät, welches in Kombination mit einer Antenne mit einem Transponder kommuniziert. Das Lesegerät besitzt eine Schnittstelle zu einem IT-System auf dem eine Middleware läuft. Über diese Middleware werden die Kommunikationsprotokolle des Lesegerätes umgewandelt und für die weitere Verarbeitung beispielsweise mit dem Library Managementsystem (LMS) aufbereitet. Ab da erfolgt die Kommunikation über die für Bibliotheken typischen Schnittstellen und Protokolle.

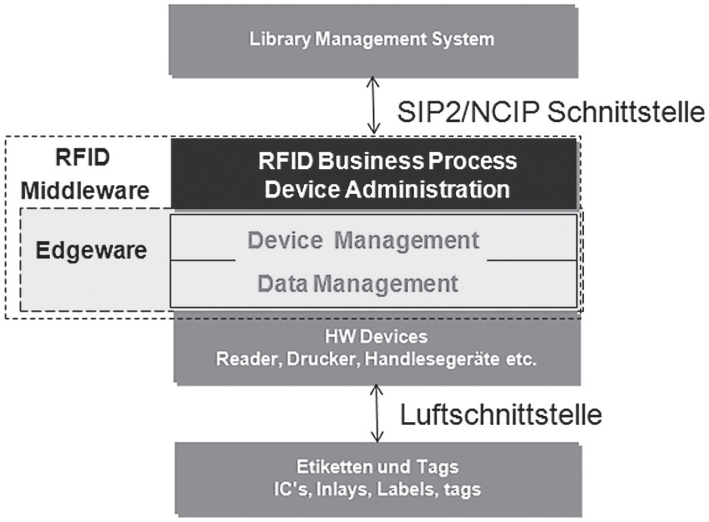


Abb. 2: Schema Teil-RFID-System in einer Bibliothek [in Anlehnung an Gill2007]

Bezüglich der Anforderungen an RFID-Systeme in Bibliotheken konnten verschieden Einflussgrößen auf die einzelnen Teilsysteme identifiziert werden. Je nach Verwendungszweck eines Teilsystems ergeben sich unterschiedlichste Bewertungskennzahlen und Einflussgrößen. In den Analysen der Teilsysteme dieses Konzeptes werden diese Parameter spezifiziert und darauf aufbauend die zu entwickelnden Prüfverfahren hergeleitet.

Definitionen Qualitätsmanagement

Unter Qualität versteht man die Gesamtheit der Merkmale und Merkmalswerte eines Produktes oder einer Dienstleistung bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen. [vgl. ISO 8402]

Voraussetzung für das zu konzipierende Qualitätsmanagement für die RFID-Nutzung in Bibliotheken sind Qualitätsstandards mit klar definierten Anforderungen an RFID-Bibliothekssysteme.

Ausgangspunkt sind die Anforderungen bisheriger Ausschreibungen hinsichtlich Funktionalität, Sicherheit, Zuverlässigkeit, Wartbarkeit, Anpassbarkeit usw. Damit die Qualität von RFID-Systemen bereits im Vorfeld und auch während der unterschiedlichen Projektphasen sichergestellt werden kann, ist eine ganzheitliche Qualitätssicherung notwendig. Diese umfasst alle geplanten und systematischen Tätigkeiten, die innerhalb eines Qualitätsmanagementsystems verwirklicht sind und die solche Qualitätsanforderungen erfüllen.

Das Qualitätsmanagement selbst umfasst dabei sowohl die Arbeitsmittel zur Erfüllung dieser Anforderungen, als auch neben der Qualitätssicherung alle Formen der Qualitätspolitik, Qualitätsplanung und Qualitätsverbesserung.

Die Abgrenzungen der einzelnen Begriffe werden in der Qualitätsmanagement-Normenreihe DIN EN ISO 9000 ff. sowie in den zu den Normen dazugehörigen Qualitätsmanagement-Elementen aufgezeigt. Die Werkzeuge und Methoden des Qualitätsmanagements lassen sich je nach Zielsetzung in Methoden und Werkzeuge zur Qualitätsplanung, zur Produktrealisierung, zur Qualitätsauswertung und zur Qualitätsverbesserung systematisieren. Diese sind jedoch komplex. In Anlehnung an die Normenreihe DIN EN ISO 9000 ff. werden daher praxistaugliche Maßnahmen vorgeschlagen, welche die Fehlererkennung und Fehlervermeidung im Bezug auf RFID-Systeme in Bibliotheken in vereinfachterem Umfang realisiert.

Für die Implementierung neuartiger RFID-Bibliothekssysteme werden in den unterschiedlichen Projektstadien unterschiedliche Qualitätssicherungsmaßnahmen (Abb. 3) benötigt. Bereits zu Beginn einer Ausschreibung (Stufe 1) sind präventive Qualitätsmanagement-Prozesse notwendig, die es ermöglichen, bereits in dieser frühen Phase wesentliche Anforderungen zu validieren. Somit lassen sich Fehler vermeiden, die später möglicherweise mit hohen Kosten verbunden sind.

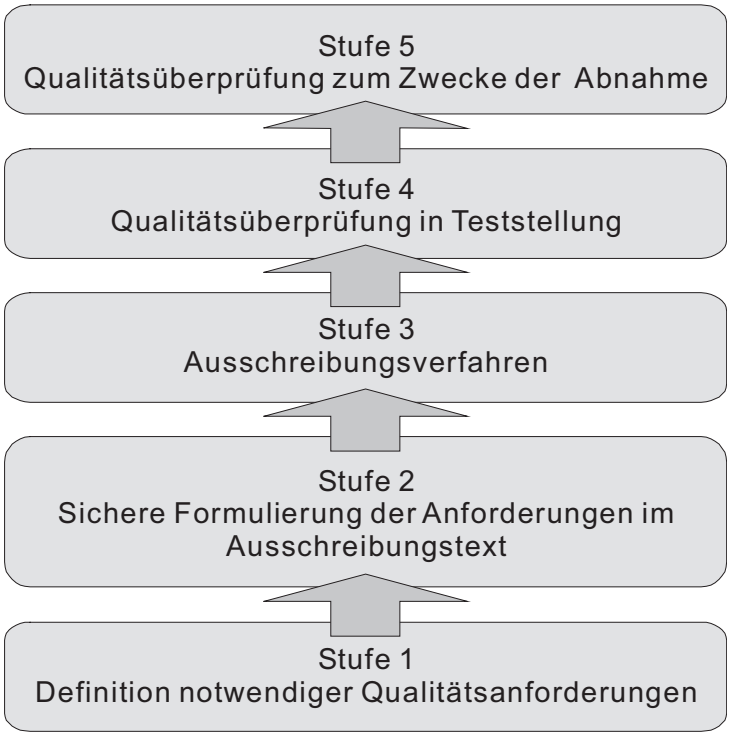


Abb. 3: Qualitätssicherungsmaßnahmen für alle Projektphasen

Um die zuvor genannten Ziele zu erreichen, wird in der ersten Stufe eine Anforderungsanalyse vorgenommen. Hier wird genau ermittelt, welche Eigenschaften bei welchem Gerät den Kann-, Soll- bzw. Muss-Anforderungen zu gerechnet werden. In der zweiten Stufe müssen die ermittelten Eigenschaften präzise und rechtssicher für die Ausschreibung festgeschrieben werden.

In der dritten Stufe ist eine Teststellung des jeweiligen Systems sinnvoll. Es erfolgt eine erste Funktions- und Leistungsüberprüfung, bei der analysiert wird, ob sich die Anforderungen der Ausschreibung (Soll-Werte) mit den Kennzahlen des Testsystems (Ist-Werte) decken und ob Eigenschaften wie in der Dokumentation zugesichert eingehalten werden. Durch vertiefende Untersuchungen des jeweiligen Systems können die Anforderungen der Ausschreibung an dieser Stelle dann noch weiter präzisiert werden.

In der vierten Stufe erfolgt dann die Auftragserteilung mit der zeitlich nachgelagerten Anlieferung der Systeme. Bei der Anlieferung unterlaufen die Geräte dann eine einfache Funktionsüberprüfung. Hier soll sichergestellt werden, dass sich die Geräte in einem, für den späteren Betrieb einwandfreien Zustand befinden. Die Prüfverfahren und Tests, die dabei zum Einsatz kommen, sind an die Praxis angelehnt.

In der fünften Stufe, der Abnahme, sollten die angelieferten Teilsysteme eindeutig identifiziert und auf besonders wichtige Merkmale und Eigenschaften hin im Detail untersucht werden. Abnahme- und Produktionsumgebung sind dabei identisch. Definierte und abgestimmte Abnahmekriterien stellen sicher, dass die vertraglichen Forderungen hinsichtlich Leistungserbringung und Funktionserfüllung im Sinne der Bibliothek bei der Abnahme von Systemteilen erfüllt werden, damit Mängel durch rechtzeitige Feststellung und Analyse von Fehlern verhindert werden können. Werden alle Anforderungen der Bibliothek hinsichtlich der realisierten Merkmale des Produktes erfüllt, gilt die Abnahme als bestanden.

Als Abgrenzung gegenüber den Prüfverfahren zur Feststellung, ob ein Prüfgegenstand eine oder mehrere vereinbarte, vorgeschriebene oder erwartete Bedingungen erfüllt, werden Tests benötigt. Diese zeichnen sich dadurch aus, dass bei ihnen in einem standardisierten Verfahren unter bestimmten definierten Bedingungen individuelle Funktions- und Spezifikationsmerkmale gemessen werden, um später Schlüsse auf die Eigenschaften und auf das Verhalten von Systemen in anderen (ähnlichen) Situationen ziehen zu können.

Der Vorgang des Messens an sich hat dabei in beiden Verfahren einen experimentellen Charakter bei der nach DIN 1319 ein spezieller Wert einer physikalischen Größe als Vielfaches einer Einheit oder eines Bezugswertes ermittelt wird.

Tests als standardisierte Verfahren haben darüber hinaus den Vorteil, dass im Fall von Meinungsunterschieden zum Erbringungsstand von Leistungen und bei Problemen bei der Abnahme, die Rechtsprechung sich erfahrungsgemäß am Stand der Technik orientiert, das heißt, in der Regel an den dazu vorliegenden Normen und Richtlinien. Dies ist ein wesentlicher Grund, weshalb die TH Wildau die Bemühungen vorantreibt, diesen Stand der Technik von RFID-Bibliothekssystemen in Form einer VDI Richtlinie (4478) zu beschreiben. Diese sollen dann mit Beurteilungs- und Bewertungskriterien fundierte Entscheidungshilfen liefern und somit den Maßstab für einwandfreies technisches Vorgehen bei der Qualitätssicherung von RFID-Systemen definieren.

Ausgehend von seiner Komplexität ist ein RFID-System als IT-System anzusehen, da es sich um ein dynamisches und technisches System mit der Fähigkeit zur Speicherung und

Verarbeitung von Informationen handelt. Es umfasst somit nicht nur die RFID-Hardware, sondern auch alle Komponenten der Hard- und Software sowie des Netzwerkes, die für die Kommunikation mit dem Library Management System (LMS) notwendig sind.

Für IT-Systeme beschreibt ISO 90003 in verschiedenen Abschnitten phasenunabhängige Aktivitäten. Besonders der Abschnitt der Integration/Systemtests bzw. Betrieb/Wartung kann hier auf die Aktivitäten der RFID-Einführung in Bibliotheken übertragen werden. Dabei kommen folgende Prüfmethoden in Betracht:

- Blackbox-Text
- Whitebox- Test
- Systemtest
- Stresstest/Lasttest
- Integrationstest
- Installationstest
- Abnahmetest
- Feldtest

Ein Blackbox-Test ist ein Testverfahren bei dem Tests ohne Kenntnisse der Implementierung vorgenommen werden. Beim gegenteiligen Whitebox-Test werden Kenntnisse über die Funktionsweise des Systems vorausgesetzt. In Bezug auf RFID-Systeme in Bibliotheken erfolgen die meisten Tests nach der Blackbox-Methode, da die inneren Strukturen und Abläufe der Systeme unbekannt sind. Lediglich die Funktions- und Wirkweise der jeweiligen RFID-Komponente kann als bekannt vorausgesetzt werden. Unter Systemtest versteht man einen Test des fertigen Systems gegen die in den Anforderungsdokumenten festgelegten Funktions-, Leistungs- und Qualitätsanforderungen. Dies setzt eine konventionelle, funktionsorientierte Testplanung voraus, in der die Testfälle auf Grundlage der Anforderungen an die RFID-Systeme entwickelt werden. Dem Systemtest unterzuordnen sind die Stress- bzw. Leistungstests, in denen Systeme hinsichtlich ihrer Funktionalität in Grenzbereichen untersucht werden bzw. deren Leistungsverhalten überprüft wird. Hier werden dieselben Anforderungen überprüft, jedoch befindet sich das System in einer Lastsituation bzw. wurden ihm Ressourcen entzogen.

Der Begriff Integrationstest bezeichnet eine aufeinander abgestimmte Reihe von Einzeltests, die dazu dienen, verschiedene voneinander abhängige Komponenten eines komplexen Systems im Zusammenspiel zu testen. Beim Installationstest wird geprüft, ob das System mit den Installationsbeschreibungen, die beispielsweise im Benutzerhandbuch dokumentiert sind, installiert und in Betrieb genommen werden kann. Ist dies erfolgreich, erfolgt meist anschließend der Abnahmetest, bei dem das System gegen die Produktdefinition getestet wird. Auftretende Fehler werden dabei in einem Abnahmeprotokoll dokumentiert. Wenn die Fehler tolerierbar sind oder korrigiert werden können, dann erfolgt die Abnahme des Systems durch den Auftraggeber. Andernfalls wird die Abnahme verschoben und das System muss nachgebessert werden.

Bei einem Feldtest handelt es sich um ein Verfahren, das die Qualität eines Produktes unter nicht manipulierbaren Realbedingungen testet. Dies ist dann der Fall, wenn das System vor Ort in der Bibliothek installiert wurde.

Zur Sicherstellung der Qualität solcher IT-Systeme bedarf es eines Qualitätsmanagements mit einer den Aufgaben entsprechend angepassten Aufbauorganisation, die für die einzelnen Projektstadien die richtigen Kompetenzen eindeutig zuordnet. Idealerweise werden die dafür beauftragten Personen der Projektleitung unterstellt und besitzen je nach Projektabschnitt leitende, ausführende, bzw. prüfende Funktion.

Prüfvorschriften und Richtlinien und Standards

Stand der Entwicklung

Unterstützt wird diese Entwicklung durch mehrere Standardisierungsinitiativen, die sich im Bereich RFID mit Standardisierungen und Normung in den Bereichen Technologie, Kommunikation, Daten und Anwendungen auseinander setzen. Standards sind dabei technisch-ökonomische Vorschriften, in denen einheitlich anzuwendende Lösungen festgelegt sind. Sie regeln, wie Systeme in Bezug auf die Qualität und zu verwendende Rohstoffe und Materialien beschaffen sein müssen, bzw. welche technischen und ökonomischen Forderungen sie erfüllen müssen; sie haben empfehlenden Charakter. Ein Standard, der auf nationaler oder internationaler Ebene durch ein Normungsverfahren als allgemein gültig und rechtlich anerkannt und veröffentlicht wird, bezeichnet man als Norm. Sie besitzt die größte Verbindlichkeit einer aufgeführten Spezifikation. Eine Norm ist eine anerkannte Regel, die insbesondere in der Technik zu einer Vereinheitlichung von Eigenschaften, Produkten oder Prozessen führen soll und dabei bestimmenden Charakter besitzt.

Daneben existieren noch weitere richtungsweisende, praktische Arbeitsunterlagen vom Verein Deutscher Ingenieure e.V. (VDI), die den Stand der Technik widerspiegeln (siehe Tabelle 1). Diese VDI-Richtlinien vereinheitlichen die Anforderungen an materielle und immaterielle Güter, schaffen Vergleichbarkeit und vermeiden Anpassungskosten. Im Bezug auf Abnahmerichtlinien bezüglich Schleusensysteme gibt es die VDI 4470 in deren Anlehnung auch die Prüfverfahren an RFID-Gates entwickelt wurden.

Technische Standards	
DIN EN 62369-1 / VDE 0848-369-1	Ermittlung der Exposition von Personen gegenüber elektromagnetischen Feldern im Frequenzbereich 0 Hz bis 300 GHz durch Geräte mit kurzer Reichweite
DIN EN 50364 VDE 0848-364	Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die im Frequenzbereich von 0 Hz bis 300 GHz betrieben werden
ISO/IEC 15691	RFID for Item Management Datenformat und Speicherung Data encoding Rules and logical Memory functions
ISO/IEC 15692	RFID for Item Management – Datenprotokoll Anwendungsschnittstelle
ISO/IEC 15693	Regelung für eindeutige Ident-Nummern (»Unique Identifier«) für Transponder beziehungsweise Tags
ISO/IEC 18000-1	Luftschnittstelle – Referenzarchitektur und Parameterbeschreibung
ISO/IEC 18000-3	Luftschnittstelle 13.56 MHz
ISO/IEC TR 24710:2005	Elementary tag license plate functionality for ISO/IEC 18000 air interface definitions – Elementartransponder

Technische Standards	
ISO/IEC 18046:2006 1/2/3	Leistungstests von RFID-Systemen
ISO/IEC 18047-3:2004	Konformität der Luft-Schnittstelle 13,56 MHz
ETSI EN 300 330	Funkparameter im Bereich 9kHz bis 30 MHz
ETSI EN 301489	Elektromagnetische Kompatibilität
VDI 4470/1	Warensicherungssysteme – Kundenabnahmerichtlinie für Schleusensysteme Ermittlung der Erkennungsrate und Detektionsrate bei der Inbetriebnahme von EAS-Systemen vor Ort
VDI 4470/2	Warensicherungssysteme – Kundenabnahmerichtlinie für Deaktivierungs-anlagen« Prüfung von Deaktivierungsanlagen für EAS-Systeme Abnahme mit realen Produkten
VDI 4470/3,4	Warensicherungssysteme – Kundenabnahmerichtlinie für Deaktivierungs-anlagen Prüfung von Deaktivierungsanlagen für EAS-Systeme Abnahme mit künstlichen Produkten
VDI 4472/2	Anforderungen an Transpondersysteme zum Einsatz in der Supply Chain – Allgemeiner Teil
VDI/AIM 4472/10	Testverfahren zur Überprüfung der Leistungsfähigkeit von Transponder-systemen (RFID)
VDI 4471	Anforderungen an Transpondersysteme zum Einsatz in der Supply Chain
VDI 4478	Anforderungen an RFID-Systeme für den Einsatz in Bibliotheken (in Arbeit)
VDI 4478-1	Testverfahren zur Vereinheitlichung der Leistungsbestimmung von RFID-Gates für den Einsatz in Bibliotheken (erschienen 2012)
VDI 4478-2	Leistungsbestimmung von RFID-Label für den Einsatz in Bibliotheken (in Arbeit)
Qualitätsstandards	
DIN 1319	Deutsche Norm in der Messtechnik – Grundbegriffe,
DIN EN ISO 9000	Grundlagen von Qualitätsmanagementsystemen
DIN EN ISO 9001	Anforderungen an ein Qualitätsmanagementsystem
DIN EN ISO 9004	Effizienz von Qualitätsmanagementsystemen
VDI 2619 1985	Prüfplanung Arbeitsschritte zur Erstellung eines Prüfplanes
DIN 32937	Mess- und Prüfmittelüberwachung
ISO /IEC 90003:2004	Software Engineering ISO 9000 für Software

Tab. 1: Standards/Normen/Richtlinien im Bereich RFID/Qualitätsmanagement

VDI Richtlinienarbeit 4478

Mit der Einrichtung eines Runden Tisches an der TH Wildau zur Erarbeitung von Prüfvorschriften zur Messung der Leistungsfähigkeit von RFID Gates Systemen (13,56 MHz) ist der Startschuss für die Erstellung offizieller VDI Richtlinien gefallen. Mit der Richtlinienrahmennummer 4478 können nun die notwendigen Beschreibungen des Stands der Technik erfolgen. Begonnen wurde mit der Betrachtung der Gatesysteme, die hinsichtlich der Funktionalität die größte technische Herausforderung darstellen.

Naturgemäß entwickeln sich Richtlinienwerke weiter und es werden andere systemrelevante Fragestellungen behandelt. So ist in der Abb. 4 ein möglicher Aufbau des Richtlinienwerkes VDI 4478 RFID Einsatz in Bibliotheken skizziert.

Für die internationale Nutzbarkeit der VDI Richtlinie ist es von Bedeutung, dass der Richtlinienausschuss international besetzt ist und eine deutsch-englische Ausgabe von Beginn zur Verfügung steht. Des Weiteren ist der Verband der Industrie der

Automatischen Identifikation und Mobilen Datenerfassung AIM e.V. bzw. dessen Mutterorganisation AIM Global mit Sitz in den USA, autorisiert, direkte Eingaben beim ISO vorzunehmen. Es wird angestrebt, den AIM für Einbringung der VDI Richtlinie in den internationalen Standardisierungsprozess zu gewinnen.

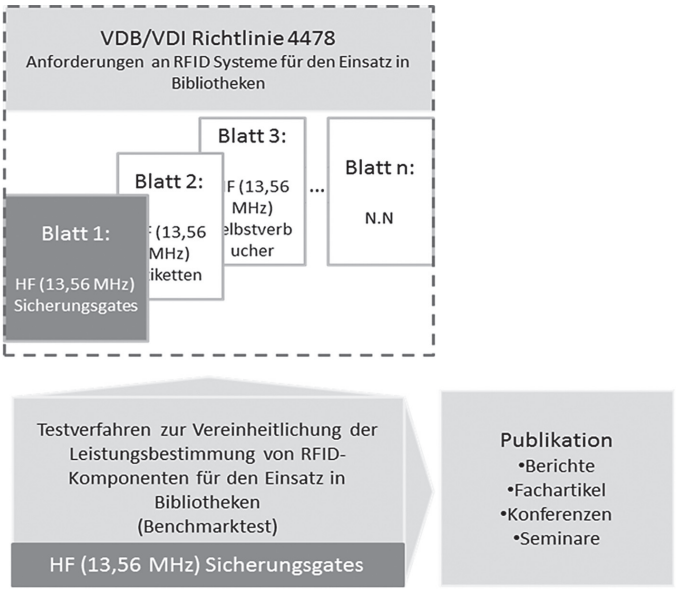


Abb. 4: Möglicher Aufbau des Richtlinienwerkes 4478

Der Nutzen derartiger Richtlinien und Standards ist eindeutig in einer Professionalisierung der Anwendung von RFID in Bibliotheken zu sehen, d. h. in der Perfektionierung des Marktes hin zu einem transparenten Markt.

Im Einzelnen können folgende Aspekte des Nutzens nach Interessensgruppen genannt werden:

Nutzen für die Anwender

Die Vorgehensweise bietet für die Anwender vielfältigen und nachhaltigen Nutzen.

- Unterstützung bei der Definition wichtiger qualitätsbestimmender Eigenschaften
- Vereinfachung von Ausschreibungen durch Bezug auf Richtlinien und Normen oder auch die Forderung von Nachweisen einer bestimmten Qualität z. B. in Form von Zertifikaten und Prüfprotokollen
- Vergleichbare Leistungsmetrik zur Unterstützung von Ausschreibungsentwürfen
- Nachweisbare Berücksichtigung des Stands der Technik, d. h. verbesserte Prüfungsfestigkeit in den Vergabeverfahren
- Einheitliche Terminologie zur verbesserten Kommunikation mit den Anbietern
- Reduzierte Einarbeitung von Personen in detaillierte technische Vorgänge
- Verlässliche Abnahmeprozeduren vor Ort
- Reproduzierbare Abläufe während der Abnahme und des täglichen Betriebs
- Schnellere Diagnose von Ursachen bei Ausfällen/Leistungsminderungen

Nutzen für die Anbieter

Die Vorgehensweise bietet für die Anbieter ebenfalls vielfältigen und nachhaltigen Nutzen.

- Vereinfachte Kommunikation von Differenzierungsmerkmalen der Produkte
- Anforderungsoptimierte Angebote für robuste Preispolitik
- Beschleunigte Vorortabnahmen führen zu geringeren Implementierungskosten
- Standardisierte Schulungen des technischen Personals der Anwender
- Tragfähige Schulungen können von Dritten angeboten werden
- Standardisierbare Diagnose-Modelle führen zu einer Optimierung des Serviceangebotes (1st, 2nd, usw. Level Support)
- Offizielle zweisprachige Richtlinien des VDI führen zur Beeinflussung auch des europäischen Marktes und führen zu Synergien
- Adaption durch ISO
- Vereinfachte Positionierung am Markt

Begriffsbestimmung

Um Medien wirkungsvoll vor Diebstahl zu schützen, werden RFID-Sicherungsgates im Zugangsbereich zur Bibliothek bzw. zu den Lesesälen installiert. Über eine Kennzeichnungsmöglichkeit auf den Transpondern können diese unterscheidbar gruppiert werden. Die Alarmgenerierung über diese Merkmale erfolgt in Deutschland meist durch Programmierung des AFI (application family identifier) auf dem Transponder. Im Zuge der Mediensicherung sendet ein Gate einen entsprechenden Abfragebefehl, auf den dann die mit dem entsprechenden AFI-Wert programmierten Transponder reagieren. Dies stellt nur die Alarmfunktionalität und die Abfrage der eindeutigen Transpondernummer (UID) sicher. Weitere Informationen zum Medium selbst müssen zusätzlich vom Transponder oder aus einer Datenbank ausgelesen werden. In anderen Regionen wird oft die Erkennung mittels EAS-Verfahren eingesetzt. Dabei reagiert jeder Transponder im Gate, bei dem die EAS-Alarmfunktion frei geschaltet wurde. Dieses Verfahren bietet zwar den Vorteil, dass die Alarmierung sicher ausgeführt wird, hat aber gleichzeitig den Nachteil, dass die UID oder andere Mediendaten nicht ermittelt werden. Es ist somit nicht unterscheidbar, ob der alarmauslösende Transponder aus der betreffenden Bibliothek stammt und auch nicht, um welche Art Medium es sich handelt. Nach der Alarmauslösung müssen also andere Prozesse folgen, um eine höhere Sicherheitsstufe zu erreichen.

Analyse der funktionsbestimmenden Parameter

Die Erkennungsrate ist das Hauptmerkmal bei der Beurteilung von RFID-Schleusensystemen. Die Erkennungsrate stellt sich dabei als Verhältnis von erfassten zu erfassbaren Transpondern dar. Sie sollte im Idealfall hundert Prozent betragen, nämlich dann, wenn immer alle Transponder detektiert werden. Dies ist jedoch in der Realität nicht immer der Fall. Aus theoretischer Sicht gibt es mehrere Faktoren, die zu einer Beeinflussung der Detektion beitragen und sich somit auf die Erkennungsrate auswirken:

Zum einen ist die Verweildauer der Transponder innerhalb des Erfassungsbereiches des Gates zu nennen; da die Transponder durch spezielle Zugriffsverfahren sequentiell gelesen werden, muss diese ausreichend hoch sein. Die notwendige Verweildauer wird wiederum beeinflusst durch die Anzahl der Transponder. Geht man davon aus, dass für die Detektion eines Transponders eine bestimmte Zeit benötigt wird, so summieren sich die Zeiten, wenn mehrere Transponder verwendet werden. Sollen zusätzlich zur AFI-Erkennung noch weitere Daten vom Transponder gelesen werden, muss die Verweildauer für das Auslesen angepasst werden.

Die Verweildauer wird durch die Geschwindigkeit bestimmt, mit der die Transponder durch den Erfassungsbereich bewegt werden. Die Verweildauer ist hier umso kürzer, je schneller die Transponder durch das Gate bewegt werden. Die Strecke, die dabei innerhalb des Erfassungsbereiches zurückgelegt wird, ist abhängig von Antennengröße bzw. von der Gate-Tiefe. Diese sind bei einem installierten Gate konstante Produktmerkmale.

Ein weiterer Faktor, der Einfluss auf die Detektion und damit Erkennungsrate hat, ist die Homogenität und die Ausbreitung des magnetischen Feldes. Eine optimale Erfassung von Transpondern kann nur dann erreicht werden, wenn zwischen zwei Gate-Antennen eine lückenlose Ausbreitung des Feldes erreicht wird, sodass an jeder Position genügend Energie bereitsteht, um Transponder mit Energie zu versorgen und eine Kommunikation aufzubauen. Auch spielt die Lage der Transponder innerhalb des magnetischen Feldes eine Rolle; je nach Bauform der Gate-Antenne baut sich um die Antennenwindungen ein charakteristisches Feld auf. Die Koppeleigenschaften von magnetisch gekoppelten Systemen hängen jedoch maßgeblich von der mechanischen Anordnung zueinander ab. Eine Neigung des Transponders gegenüber den Feldlinien vermindert die Durchdringung der Transponderspule durch die Feldlinien des Gates und es kann im ungünstigsten Fall keine Energieversorgung beziehungsweise keine Kommunikation mehr stattfinden. Deshalb ist es wichtig, Prüfverfahren zu entwickeln, welche die Lage von Transpondern berücksichtigen. Damit der Aufwand noch akzeptabel ist, werden für einen Transponder die 12 wichtigsten möglichen Lagen definiert (Abb. 4). Ausgehend von einem dreidimensionalen kartesischen Koordinatensystem sind dies 6 Hauptlagen und weitere 6 Hauptlagen, die jeweils um 45° gedreht wurden.

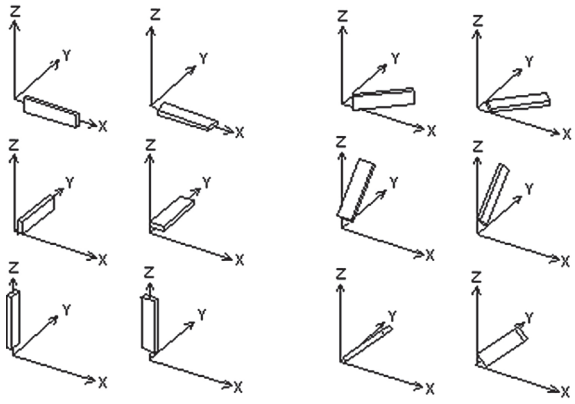


Abb. 4: Darstellung der 12 Transponderlagen [VDI4470]

Die Homogenität des Feldes kann beeinträchtigt werden, wenn der Abstand der Gate-Antennen so groß ist, dass eine vollständige Durchflutung des Durchgangsbereiches nicht mehr erreicht werden kann. Die Reichweite der Antennen von Gates ist deshalb ein prüfenswerter Parameter.

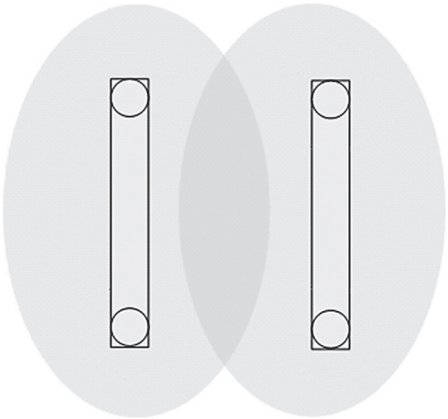


Abb. 5: Feldhomogenität bei einem RFID-Gate (Draufsicht)

Eine optimaler Antennenabstand, wie vom Hersteller empfohlen, kann in den Bibliotheken aufgrund von baulichen und architektonischen Restriktionen sowie Vorschriften nicht immer realisiert werden. Typische Durchgangsbreiten von Gates innerhalb der Bibliotheken bewegen sich daher in Bereichen zwischen 90 und 120 cm. Bei großen Abständen als vom Hersteller des Gates vorgegeben können jedoch Lücken im Detektionsbereich auftreten, in denen eine Detektion von Transpondern nicht mehr möglich ist. Prüfverfahren, bezüglich der Durchgangsbreite müssen daher die gegebenen Antennenabstände vor Ort berücksichtigen.

Die Hauptfunktion eines RFID-Sicherungsgates, die Mediensicherung, sollte auch im Sinne des Diebstahlschutzes getestet werden. Dabei sollte die Diebstahlsituation so geprüft werden, wie sie auch in der Realität ablaufen würde. Die Auswahl der Medien und der Transportverstecke sollte typischerweise heterogen erfolgen und sich an bereits bekannten Diebstählen aus dem Bibliotheksalltag orientieren. Diebstahlstatistiken, sofern erfasst, könnten dabei wichtige Kennzahlen liefern.

Eine optional vorhandene Besucherzählung muss hinsichtlich der Erkennungsrate untersucht werden, da sie die Genauigkeit der Zählfunktion widerspiegelt.

Zusammenfassend ergeben sich für das Teilsystem RFID-Gate folgende qualitätsbestimmende Parameter:
- Feldhomogenität
- Pulkfähigkeit
- Erkennungsrate in Abhängigkeit der Geschwindigkeit
- Erkennungsrate in Abhängigkeit der Transponderlage
- Diebstahlschutz
- Erkennungsrate / Besucherzählung

Umsetzung der Prüfverfahren

Hintergründe

Nach der Analyse der wesentlichen Parameter ist es notwendig Prüfverfahren zu entwickeln, die folgende Eigenschaften besitzen:
- Lieferung von wiederholbaren Ergebnissen unter gleichen Umweltbedingungen (Reproduzierbarkeit)
- Nachvollziehbarkeit der Ergebnisse und Zusammenhang mit der Praxis
- Generierung eines breiten wahrnehmbaren Spektrums der Ergebnisse von unterschiedlichen Prüflingen
- Trennung der zu untersuchenden Faktoren
- kurze Testzeit
- geringer Testaufwand
- Akzeptanz durch die relevanten Marktteilnehmer
- große Präzision als Labortest
- gute Ableitbarkeit von Tests für die reale Umgebung vor Ort

Diese Eigenschaften oder besser Anforderungen an die Testprozeduren lassen sich in der Realität nicht vollständig erfüllen. Ein Beispiel: Theoretisch ist zwar eine gute Trennung der zu testenden Eigenschaften möglich, das würde aber zu einer Vielzahl von Einzeltests führen, was den Aufwand schnell in unrentable Höhen geraten lässt. Hinzu kommt noch, dass eine detaillierte Austestung von abgegrenzten Eigenschaften zwar für Hersteller oder Entwickler interessant, aber die praktische Relevanz für die Schaffung einer Entscheidungs- und Diagnosehilfe fragwürdig ist.

Zum optimalen Erreichen der o. g. Eigenschaften der Prüfverfahren ist es notwendig, Expertenwissen aus einer repräsentativen Anzahl von Marktteilnehmern zu bündeln. Dafür wurde, wie oben bereits erwähnt, an der TH-Wildau der Runde Tisch Bibliothekssysteme gebildet. Gleichzeitig wurde aktiv Kontakt zur Gruppe der Anwender von RFID-Bibliothekssystemen aufgenommen.

Über einen hinreichenden Zeitraum wurde dann ein Optimum an Tests für RFID-Sicherungsgates erarbeitet. Die in der VDI-Richtlinie VDI 4478-1 festgeschriebenen Verfahren stellen eine Gesamtheit dar. Sie bieten einen optimalen Überblick über die Qualität der getesteten Gates, sind von einer repräsentativen Menge von Marktteilnehmern akzeptiert, liefern gut gefächerte Ergebnisse und sind aufwandoptimiert.

Für diese Optimierung war es erforderlich, Abstriche an die Trennung der einzelnen qualitätsbestimmenden Merkmale zu machen. Es sind die folgenden Einzeltests definiert:
- Bestimmung von elektrischen Feldparametern zur Festschreibung des Zustandes des Prüflings während des Tests
- Bestimmung der Homogenität des Erfassungsfeldes über die Fläche des Durchgangsbereiches
- Bestimmung der Detektionszuverlässigkeit mit 18 Transpondern bei verschiedenen Geschwindigkeiten

– Bestimmung der Möglichkeit Transponder von Medienstapeln zu detektieren
– Untersuchung der Stabilität der Erkennungsrate unter dem Einfluss von aktiven und passiven Störern

Diese Einzeltests sind für die Detektionsverfahren mittels AFI und EAS definiert und entsprechend angepasst. Bei der Optimierung der Einzeltests wurde der Reproduzierbarkeit eine sehr hohe Priorität eingeräumt. Diesem Kriterium und auch der Praxisnähe sind einige anfangs vorgeschlagene Tests zum Opfer gefallen.

Eingangs wurden in der Richtlinie die einzusetzenden Prüfkörper und das nötige Testumfeld beschrieben.

Um die definierten Prüfungen effizient und wiederholgenau durchführen zu können, wurde an der TH-Wildau eine Bewegungsapparatur entwickelt und hergestellt. Sie ist in der Lage verschiedene Prüfkörper wiederholgenau mit hinreichender Präzision in Geschwindigkeit, Bahn und Lage durch das zu prüfende Gate zu verfahren. Die Bewegungen werden dabei ferngesteuert vom Prüfarbeitsplatz veranlasst.

Die Abmessungen der Apparatur sind mit 4 m x 3 m x 2,5 m deutlich größer als die des Prüflings selbst. Es ist schließlich sicher zu stellen, dass die Prüfkörper unter Beachtung des Beschleunigungs- und Bremsweges innerhalb des Erfassungsbereiches des Gates die vorgegebene Geschwindigkeit besitzen.

Der Aufbau der Apparatur erfolgte aus Nichtmetallen. Dadurch ist sichergestellt, dass die Eigenschaften des Prüflings während der Prüfung nicht durch das Hilfsmittel verändert werden.

Bei der elektrischen Verkabelung wurde darauf geachtet, dass der Prüfling nicht von Fremdfeldern beeinflusst wird.

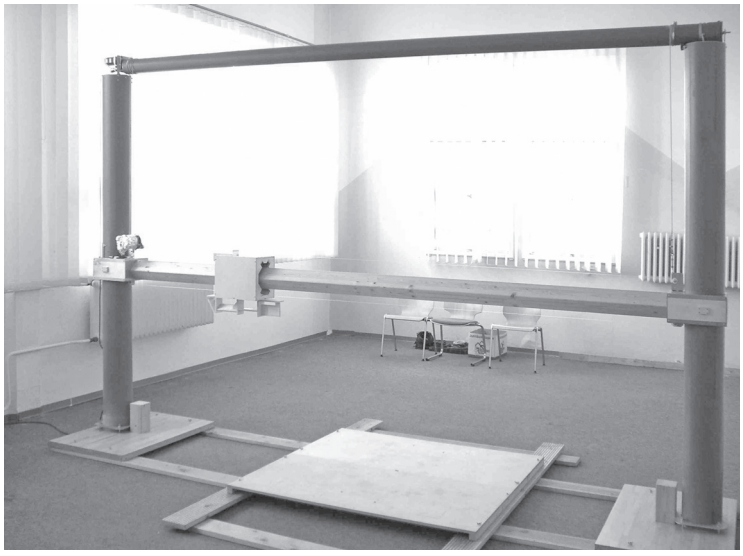


Abb. 6: Bewegungsapparatur

Homogenität des Erfassungsfeldes

Für diesen Test wurde ein Prüfkörper definiert, der aus 5 Transpondern besteht, die gut abgestimmt sind und sich hintereinander in einer Linie in verschiedenen Ausrichtungen befinden. Dieser Prüfkörper wird auf einer größeren Anzahl genau definierter Verfahrlinien mit einer definierten Geschwindigkeit durch das Gate bewegt. Man erhält Aussagen darüber, wie gut das Erfassungsfeld innerhalb des Gates über den Durchgangsbereich verteilt ist.

Detektionszuverlässigkeit

Dieser Test wird mit einer größeren Anzahl von Transpondern (18 Stück) innerhalb des Prüfkörpers mit unterschiedlichen Geschwindigkeiten durchgeführt. Er stellt die Eigenschaften des Gates unter erhöhter Belastung dar. Durch den Einsatz von unterschiedlichen Geschwindigkeiten wird deutlich, ob sich ein Gate z. B. an seiner Leistungsgrenze befindet. Um die Reaktion des Gates unter »Belastung« auf unterschiedliche Transponderausrichtungen festzustellen, wird der Prüfkörper in drei verschiedenen Ausrichtungen durch das Gate verfahren. Die Anzahl der Verfahrlinien wurde zur Verkürzung der Testzeit reduziert.

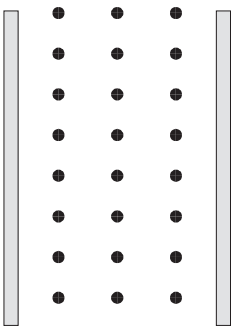


Abb. 7: Verfahrlinien

Stapelleistung

Hier wird untersucht, wie das Gate mit einer Vielzahl von Transpondern arbeitet, die ähnlich der Realität durch unterschiedliche Arten von Medien und unterschiedliche Nähe zu anderen Transpondern verstimmt sind. Dazu wurde zunächst eine Anzahl von üblichen Büchern ausgewählt; es wurde also bewusst auf Bücher mit Metalleinband oder ähnliche Exoten verzichtet. Anschließend wurden die maßgeblichen Eigenschaften dieses Stapels bestimmt und ein Prüfkörper definiert, der diese Eigenschaften repräsentiert und aus einfachen wieder beschaffbaren Mitteln hergestellt ist. So ist dafür Sorge getragen, dass auch diese Prüfung unabhängig von der Beschaffbarkeit bestimmter Medien zu späteren Zeitpunkten reproduzierbare Ergebnisse liefert.

Abb. 8: Buchstapel

Störfestigkeit, aktiver Störer

Zunächst wird die Erkennungsrate des zu prüfenden Gates bestimmt. Dann wird aus großer Entfernung ein definierter Störer (eingeschalteter RFID-Reader) mit festgeschriebener Feldstärke sukzessive dem zu prüfenden Gate angenähert. In den jeweiligen Entfernungsstufen wird die Erkennungsrate wiederholt bestimmt. Das Ergebnis des Tests ist die Entfernung des Störers, bei der das Gate noch die gleiche Erkennungsrate liefert wie bei der ersten Referenzbestimmung.

Diese Untersuchung liefert Erkenntnisse über die Robustheit gegenüber Feldern von anderen RFID-Geräten, die u. U. in der Nähe des Gates installiert werden. Das Ergebnis ist jedoch nicht zu verwechseln mit der Ermittlung einer minimalen Entfernung für die geplante Installation eines RFID-Gerätes; hierfür sind weitere Gesichtspunkte heran zu ziehen.

Störfestigkeit, passiver Störer

Wird ein Gate sehr dicht an einem metallischen Element, z. B. an einem bauseitig vorhandenen Stahlträger oder einem metallischen Türrahmen installiert, wird ein Teil der Feldenergie, die zum Versorgen der Transponder erzeugt wird, in dem metallischen Element in Wärme umgesetzt. Sie geht also den Transpondern verloren. Gleichzeitig wirkt dieses Metall verstimmend auf die resonanten Gate-Antennen. Sie können also nicht so unbeeinflusst arbeiten wie in einer metallfreien Umgebung.

Für diesen Test wurde ein Prüfkörper aus Stahlblech definiert, der das Vorhandensein von Metall simulieren soll. Er wird in Schritten an das Gate heran gebracht, wobei wie beim zuvor beschriebenen Test jeweils die Erkennungsrate bestimmt wird. Die Entfernung, bei der die Erkennungsrate gerade noch der Referenzmessung entspricht, stellt das Ergebnis dar. [vgl. VDI 4478-1]

Anhang

Beispiel möglicher Abläufe bei der Beschaffung von RFID-Sicherungsgates

Die Beispiele beziehen sich auf die Beschaffung innerhalb von Deutschland. Hier kommen meist Gates um Einsatz, die auf Basis des Detektionsverfahrens »AFI« die Transponder der Medien detektieren. Bild A1 zeigt ein Schema mit zwei Ablaufvarianten. Nach der ersten Variante wird die Durchgangsbreite zwischen den einzelnen Antennen vom der ausschreibenden Stelle fest vorgegeben. Die Anbieter bieten entsprechend viele Antennen an, damit die Gesamtdurchgangsbreite von z. B. 12 Metern gesichert werden kann. In der Ausschreibung wird lediglich das Zertifikat nach VDI4478-1 verlangt. Nach dessen Vorlage werden die eingehenden Angebote berücksichtigt.

Im zweiten Beispiel ist frei gestellt, wie viel Antennen der Anbieter zur Abdeckung der Gesamtdurchgangsbreite von 12 m installieren möchte. Das ermöglicht den Aufwand zu reduzieren und den technischen Möglichkeiten entsprechende größere Durchgangsbreiten zwischen den Antennen zu bekommen. Die Anbieter müssen dazu ein Zertifikat für die ggf. größere Durchgangsbreite zwischen den Antennen vorlegen. Dafür ist bei ihnen eine Zertifizierung notwendig, die über die übliche Zertifizierung für 1 m Durchgangsbreite hinaus geht. Wenn sie entsprechende Produkte liefern können, werden sie Interesse daran haben, die entsprechenden Zertifikate vorliegen zu haben.

Der Ablauf nach Bild A2 (drittes Beispiel) beschreibt das Vorgehen für Fälle, bei denen bestimme Eigenschaften der zu beschaffenen Sicherungsgates besonders hoch einzustufen sind. In diesen Fällen ist es ratsam die Richtlinie VDI4478-1 vor der Definition der

zu priorisierenden Werte zu beschaffen. Hierzu ist mit dem VDI Kontakt aufzunehmen. Der Gründruck (erste Veröffentlichungsstufe) ist hier bereits ausreichend. Da das Zertifikat, welches Unternehmen erhalten, die ihre Gates nach VDI4478 testen lassen, nur ausweist, dass die derzeit gültigen Schwellwerte aller Prüfungen mindestens erreicht wurden, ist es in diesem Beispiel notwendig das Messprotokoll in der Ausschreibung zu verlangen. Hieraus lassen sich die Ergebnisse der Teiluntersuchungen erkennen. Ist z. B. ausgeschrieben, dass das angebotene Gate im Test »Stapelleistung« besonders gute Ergebnisse bringen soll, kann das anhand des Messprotokolls überprüft werden.

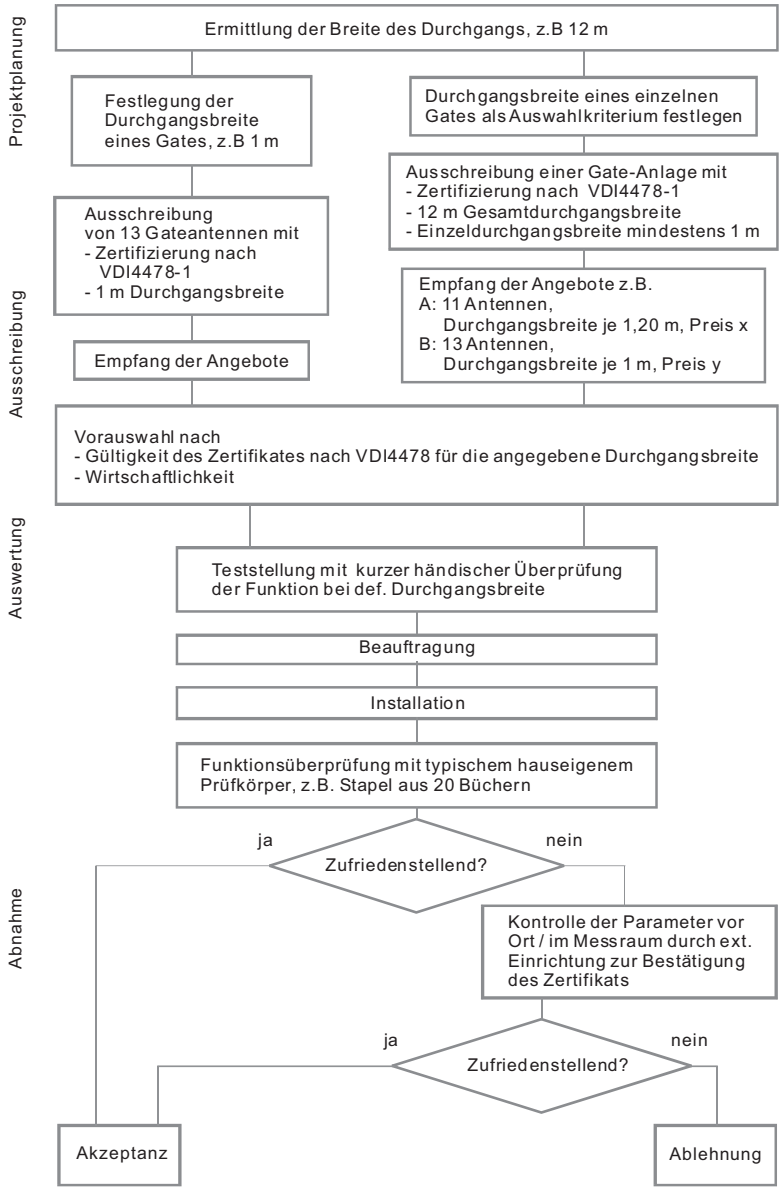


Abb. A1

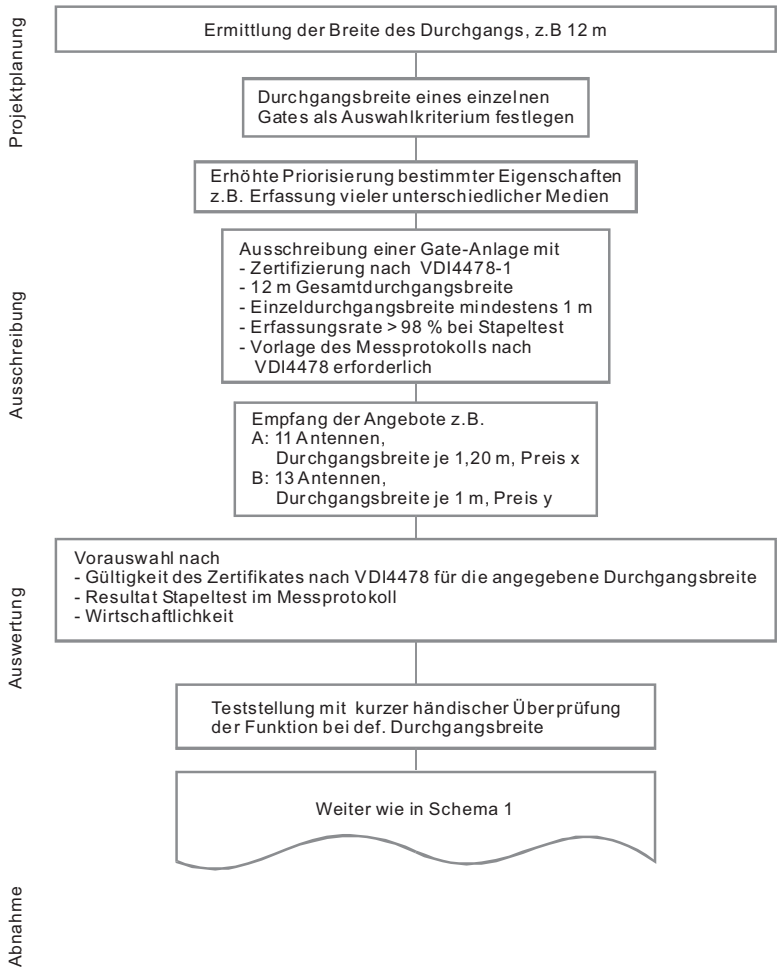


Abb. A2

Quellenverzeichnis

[Gill2007] Frank Gillert, Wolf-Rüdiger Hansen, »RFID für die Optimierung von Geschäftsprozessen«, Carl Hanser Verlag München, 2007

[ISO 8402] »Quality management and quality assurance – Vocabulary«

[VDI 4470] »Warensicherungssysteme Kundenabnahmerichtlinie für Deaktivierungsanlagen«

[VDI 4478-1] »Testverfahren zur Vereinheitlichung der Leistungsbestimmung von RFID-Gates für den Einsatz in Bibliotheken«

Abschirmungseffekte und andere Störungen

Hardy Zissel

Im Umgang mit RFID kommt es hin und wieder zu Situationen, in denen bestimmte Transponder nicht identifizierbar sind. Für derartige Effekte hat sich der Begriff »Abschirmung« im Sprachgebrauch etabliert.

In diesem Beitrag werden einige dieser zur Abschwächung des Magnetfeldes führender Effekte und der Begriff »Abschirmung« in Bezug auf den Faradayschen Käfig aus physikalischer Sicht betrachtet. Über das Verständnis dieser Effekte sollen dem Leser auch Möglichkeiten zur nachhaltigen Begegnung in der Praxis gegeben werden. Betrachtet werden hier HF-RFID-Systeme, die auf der Basis von rein magnetischer Kopplung arbeiten.

Abschirmung physikalisch

Mit dem Phänomen der Abschirmung, wie sie heute in der Regel von Technikern verstanden wird, hat sich bereits der englische Physiker Michael Faraday (1791-1867) befasst. Sie beruht auf dem Effekt, dass in der geschlossenen elektrisch leitenden Hülle einer Box durch zeitlich veränderliche Magnetfelder Wirbelströme entstehen, die ihrerseits Magnetfelder ausbilden, die den ursprünglichen Feldern entgegenwirken. Dadurch bleibt das innere der Box feldfrei. Da der Effekt auf Wirbelströmen basiert wird klar, dass er umso mehr wirkt, je schneller die zeitliche Varianz des Feldes erfolgt. Anders herum bedeutet das, dass Magnetfelder, die zeitlich konstant sind oder sich nur sehr langsam verändern, nicht von der elektrisch leitenden Hülle abgeschirmt werden.

Anders ist das allerdings bei magnetisch leitfähigen Materialien wie z.B. eisenhaltige Stoffe. Hierbei wird der Magnetfluss im Material entlang geleitet und somit aus dem Zentrum der Box »gezogen«. Wie weit dieser Effekt ausgeprägt ist, hängt von der magnetischen Leitfähigkeit und anderen magnetischen Eigenschaften (→ Hystereseverluste) des Materials ab.

Wird das Gebilde der geschlossenen Box aus leitendem Material unter der Einwirkung von elektromagnetischen Wellen betrachtet, sieht die Wirkung noch drastischer aus. Das Innere der Box ist hier feldfrei sofern die Box für die betrachtete Frequenz tatsächlich dicht ist. Das ist immer dann der Fall, wenn sie keine Durchbrüche enthält, deren Abmessungen größer als ein Viertel der Wellenlänge sind. Dabei ist allerdings die Tiefe des Durchbruchs, also die Materialdicke, noch für die Dämpfung relevant. Da das Viertel der Wellenlänge bei HF etwa 5,5 m beträgt, ist dieses Phänomen allerdings erst im UHF Bereich relevant. Hier liegt das Viertel der Wellenlänge in der Größenordnung von 5,5 cm.

Es wird deutlich, dass Abschirmungseffekte stets mit einer Box zu tun haben, deren Inneres betrachtet wird. Diesen Aufbau findet man in der Bibliothekswelt nur in Ausnahmefällen. Dennoch sind Abschwächungseffekte oft anzutreffen. Einige werden im Folgenden behandelt.

Abschwächungseffekte aus der Praxis

Aus der Voraussetzung zur Identifizierung von RFID-Transpondern kann leicht ableitet werden, an welchen Stellen im Prozess Störungen greifen und wirksam werden können. Zur reproduzierbaren Bestimmung der Robustheit z.B. einer Gate-Antenne gegen derartige Beeinflussungen, sind vereinheitlichte Beschreibungs- und Messverfahren in der VDI-Richtlinie 4478-1 definiert [VDI 4487-1].

Um einen Transponder zu identifizieren sind zwei wesentliche Bedingungen notwendig.

1. Der Transponder-Chip muss mit ausreichend Energie versorgt sein um arbeiten (Signale auswerten und Signale versenden) zu können.
2. Die Kommunikation zwischen Lesegerät (RFID-Reader) und Transponder muss störungsfrei verlaufen.

Die zweite Bedingung kann nur erfüllt sein, wenn die erste bereits erfüllt ist. Auf sie wird zuerst eingegangen.

Die Kommunikation

Um nicht zu tief in die Details der Informationsübertragung mittels Magnetfelder einzusteigen wird hier nur davon ausgegangen, dass die zu übertragenden Informationen in Einsen und Nullen zerlegt (codiert) übertragen werden. So gibt der Reader einen Befehl an die im Feld befindlichen Transponder, ihre eindeutige Nummer mitzuteilen. Anschließend antwortet der erste Transponder mit dieser Nummer und danach schließen sich sequentiell die nächsten im Feld befindlichen Transponder an.

Damit nun die jeweilige »Gegenstelle«, also zunächst die Transponder und dann der Reader die gesendeten Informationen eindeutig verstehen können, ist es notwendig, dass die gesendeten Einsen und Nullen in der vom Sender gewünschten Reihenfolge vom Empfänger verstanden werden. Deshalb gibt es innerhalb des Systems Reader – Transponder eindeutige Regeln, die festlegen, wer wann senden darf. Ein Transponder sendet stets nur nach Aufforderung durch den Reader. Der Reader steuert den Kommunikationsprozess.

Wenn der Reader die im Feld befindlichen Transponder zum Übertragen ihrer eindeutigen Nummer (UID) auffordert, ist er der einzige Sender. Durch über diese Betrachtungen hinausgehende Algorithmen ist sichergestellt, dass die Transponder geordnet sequentiell antworten. Bei dieser Antwort ist dann auch jeder einzelne Transponder der einzige Sender.

Wenn man sich vorstellt, dass der Inhalt der zu übertragenden Information von der richtigen Reihenfolge von Einsen und Nullen abhängt, kann man leicht nachvollziehen, dass es zu Missverständnissen kommt, wenn auch nur eine einzige Eins oder Null »verloren geht«, also nicht verstanden wird. Für diesen Fall sind Algorithmen zur Plausibilitätsprüfung in Reader und Transponder implementiert. Nur wenn nach Ablauf einer Prozedur zur Plausibilitätsprüfung festgestellt wird, dass die empfangene Information gültig ist, wird sie interpretiert und verarbeitet.

Dies hat zur Folge, dass die jeweilige Gegenseite nicht reagiert, wenn auch nur eine Eins oder Null verloren gegangen ist. Der Anwender kann dies als Abschirmung empfinden

und beschreibt es im Allgemeinen auch so. Die physikalisch richtige Erklärung ist allerdings meist eine andere.

Um eine Eins zu übertragen, ist genau wie für eine Null eine jeweils eindeutig definierte Signalfolge erforderlich. Diese Signalfolge besteht aus unterschiedlichen Signalen genau definierter Frequenzen. Gibt es also in der Nähe der Antennen Störer, die Frequenzen aussenden, die denen der Kommunikation sehr ähnlich sind, so bekommt der Empfänger der Information Signale mit unterschiedlichen Aussagen zur gleichen Zeit. Da er, anders als z.B. das menschliche Ohr, nicht die Richtung der Signalquellen unterscheiden kann, kann er das Nutzsignal vom Störer nicht trennen. Er kann also nicht mit Sicherheit »entscheiden«, ob er gerade eine Eins, eine Null oder nur eine Störung empfangen hat. Sollte die Entscheidung nun also falsch ausfallen, wird die empfangene Information für ungültig erklärt und es erfolgt keine Reaktion. Im Extremfall kann es mit sehr geringer Wahrscheinlichkeit auch dazu kommen, dass viele falsch interpretierte Einsen und Nullen zu einer empfangenen Information führen, die in der Plausibilitätsprüfung für gültig erkannt wird. Dadurch kann es dann zu falschen Reaktionen des Empfängers führen.

Als Sender derartiger Störsignale kommen grundsätzlich alle Systeme in Frage, die in der Lage sind, magnetische Felder mit Frequenzen im Arbeitsbereich des RFID-Systems für sehr kurze Zeit abzugeben. Es reicht schließlich aus nur eine Eins oder eine Null zu stören. Grundsätzlich kommen als störende Systeme alle Geräte in Frage, in denen elektrische Ströme fließen. Man beachte bitte, dass auch das Ein- oder Ausschalten einer Kaffeemaschine Felder im Arbeitsbereich von RFID-Systemen erzeugen kann. Derartige Felder sind allerdings von sehr kurzer Dauer. Wenn ein Transponder dabei nicht erkannt wird, so wird er gleich einige Millisekunden später bei der nächsten Abfrage erkannt. Zu einer nachhaltigen Störung kann es allerdings kommen wenn elektrische Geräte zyklisch derartige Impulse abgeben. Besonders prädestiniert sind dafür andere RFID-Geräte, deren Reichweite in das betrachtete Feld hinein reicht. Dabei ist zu bedenken, dass der Reader sehr empfindlich ist um die schwachen Signale der zu identifizierenden Transponder zu erkennen. Reicht das Feld eines anderen Readers in das betrachtete Erkennungsfeld hinein, kann es zu Störungen kommen, mit denen zunächst nicht gerechnet wird, da dieser fremde Reader keine Transponder lesen kann, die sich in der Nähe des betrachteten Readers befinden. Dennoch wird das Feld dieses störenden Readers von dem hoch empfindlichen Empfänger des betrachteten Readers »wahrgenommen«.

Die Energieversorgung

Kommen wir nun zu der ersten Bedingung, die für die Identifizierung von Transpondern erfüllt sein muss. Die Energieversorgung des Chips.

Ein elektronisches System benötigt für seine Funktion elektrische Energie. Die Transponder, die in Bibliotheken verwendet werden, verfügen über keine eigene Energieversorgung. Sie sind darauf angewiesen, dass sie in dem Moment in dem sie arbeiten sollen genügend Energie zugeführt bekommen. Diese ist nur aus dem wechselnden Magnetfeld der Reader-Antenne zu beziehen. Es induziert in der Spule des Transponders (dessen

Antenne) eine elektrische Spannung. Diese Spannung wird im Transponder-Chip gleichgerichtet und als Versorgungsspannung für seine Baugruppen verwendet. Nebenbei wird mit dem Wechselfeld auch die Information übertragen.

Ergänzend muss erwähnt werden, dass bei HF-RFID die Antennen von Reader und Transponder Elemente von resonanten Schwingkreisen sind. Es gibt also in beiden Systeme noch kapazitive Elemente, die mit den Antennenspulen verbunden sind. Durch diesen Aufbau wird die Energieübertragung wesentlich effektiver gestaltet und es sind größere Reichweiten erzielbar.

Neben dem Gewinn an Reichweite wird durch diesen Aufbau aber auch ein Nachteil erzeugt. Der Gewinn an Reichweite entsteht nur dann, wenn die Anordnung aus Induktivität (Spule) und Kapazität (Kondensator) hinreichend genau auf der Arbeitsfrequenz resonant ist.

Es sind also für die Betrachtung der Störungsmöglichkeiten der Energieübertragung mehrere elektrische Größen zu betrachten. Letztlich ist zwar nur die induzierte Spannung im Transponder ausschlaggebend, diese ist aber maßgeblich von verschiedenen anderen Dingen bestimmt.

Die Antenne des Readers muss die erforderliche magnetische Feldstäke generieren. Das geschieht, sobald durch sie ein hinreichender elektrischer Strom fließt. Dieser fließt, wenn die Ausgangsleistung des Readers groß genug ist und der Resonanzpunkt des Systems »Antenne – Kondensator« hinreichend in der Nähe der Arbeitsfrequenz liegt.

Zusätzlich wird deutlich, dass sich eine nicht so gute Resonanz mit einer höheren Reader-Leistung kompensieren lässt. Es ist also für die Betrachtung der Feldstärke des Reader-Feldes nicht ausreichend, allein die Leistung des Readers zu betrachten.

Die Antenne des Transponders muss hinreichend gut von dem Magnetfluss der Reader-Antenne durchflossen sein. Das ist der Fall, wenn die mechanische Anordnung der beiden Antennen (Reader und Transponder) zueinander optimal und der Abstand nicht zu groß ist. Die meiste elektrische Energie erhält der RFID-Chip wenn die Resonanzfrequenz der Transponder-Antenne (System aus Antennenspule und Kondensator) optimal auf der Arbeitsfrequenz abgestimmt ist.

Diese Betrachtung zeigt nicht nur die Wirkungskette auf sondern stellt auch die Punkte heraus die, bedingt durch äußere Einflüsse, Veränderungen unterliegen.

Die resonante Reader-Antenne

Die Reader-Antenne ist ein, je nach Hersteller und Antennentyp, mehr oder weniger resonantes System, was fest installiert und dabei an seine Umgebung angepasst ist. Das bedeutet, dass der Resonanzpunkt optimal auf die Arbeitsfrequenz abstimmbar ist. Da dieser Vorteil im Interesse einer optimalen Funktion auch von den Systemhäusern genutzt wird, sind die elektrischen und dielektrischen Einflüsse im unmittelbaren Umfeld der Antenne in der Bestimmung des Resonanzpunktes berücksichtigt. Wird nun

im Betrieb das Umfeld der Antenne verändert, z.B. durch eine Person, die sich direkt in der Nähe der Antenne aufhält oder durch ein neues Möbelstück oder eine Pflanze, die nach dem Abgleich (Anpassen der Antenne an ihr Umfeld) unmittelbar an der Antenne platziert wird, wird ihr Resonanzpunkt verschoben. Das bedeutet, dass die Antenne an Empfindlichkeit verliert. Das wiederum kann dazu führen, dass Transponder von ihr schlechter erfasst werden können. Dieser Effekt des Empfindlichkeitsabfalls wird in der Praxis von Laien oft fälschlicher Weise als Abschirmung bezeichnet. Schließlich sieht es so aus, als ob eine Person, die zwischen Gate-Antenne und Transponder gelangt verhindert, dass das Magnetfeld seine Gegenstelle erreicht.

Die resonante Transponder-Antenne

Das gleiche trifft auf die Transponder-Antenne zu. Ihr Resonanzpunkt verschiebt sich, wenn ihr elektrisches oder dielektrisches Umfeld verändert wird. Das führt meist dazu, dass ihre Empfindlichkeit negativ beeinflusst wird. Veränderungen sind das Einkleben in Medien mit nicht vorhergesehenen Materialien, wie z.B. Metallanteile oder massive Kunststoffeinbände. Die Annäherung eines Transponders an einen anderen führt gleichfalls zur Verschiebung des Resonanzpunktes beider Antennen.

Metallische Störer

Es gibt noch einen Effekt, der fälschlicherweise in der Umgangssprache mit Abschirmung bezeichnet wird. Hierbei handelt es sich um die Leistungsreduzierung von Antennen bei der Annäherung an metallische Gegenstände. Tatsächlich wird hierbei zum einen, wie eben beschrieben, der Resonanzpunkt verschoben und somit die Empfindlichkeit reduziert. Dieser Effekt ist allerdings korrigierbar. Zum anderen findet aber auch eine Umleitung des Magnetflusses durch dieses Metall statt. Wenn es sich um ferromagnetische Werkstoffe, also um eisenhaltige Materialien, handelt, wird der Magnetfluss in diesem Material besser geleitet als in der Umgebungsluft. Dadurch wird die im Erkennungsfeld der Antenne benötigte Energie »umgeleitet« und verliert an der wichtigen Stelle an Wirkung. Bei Metallen im Allgemeinen kommt es zusätzlich auf Grund der elektrischen Leitfähigkeit im Material zur Indizierung eines Stromflusses. Dieser Stromfluss erzeugt wieder ein Magnetfeld welches wieder einen Stromfluss indiziert. Das setzt sich fort. Dieser Effekt wird als Wirbelstrom bezeichnet. Er führt zur Umwandlung der magnetischen Energie in Wärmeenergie. Es wird also Energie aus dem Wirkungsfeld der Antenne »vernichtet«. Wie bei der Gate-Antenne tritt dieser Effekt auch im Umfeld der Transponder-Antenne auf. Da hier die Energiemenge bedeutend geringer ist, reicht bereits eine dünne Aluminiumfolie aus um die Arbeit eines Transponders unmöglich zu machen. Auch dies ist im physikalischen Sinne keine Abschirmung.

Der Gewinn für die Praxis

Wobei helfen uns diese Gedanken nun in der Praxis? Es ist nicht nur wichtig im Interesse der Verständigung treffende Begriffe zu verwenden sondern das Wissen um die

Hintergründe dieser Effekte hilft bei Überlegungen zur Verbesserung der Funktion von RFID-Systemen.

Es gibt behebbare und nicht behebbare Effekte. Die Einteilung ist weitestgehend klar. Effekte, die zur Verschiebung des Resonanzpunktes führen sind meist korrigierbar. Man benötigt »nur« die entsprechende »Stellschraube« dafür. Diese ist bei Gate-Antennen meist sogar in Form einer veränderlichen Kapazität direkt vorhanden. Bei Transpondern ist das schwieriger. Ihre Eigenschaften werden bei der Herstellung weitestgehend festgelegt. Die Bibliothek hat hier keinen wirtschaftlich vertretbaren Einfluss. Wenn allerdings den Herstellern von Gate-Antennen und Transpondern Möglichkeiten zur Verfügung stünden, die Resonanz nur gering nutzen zu müssen, also die Resonanzkurve flach (die Kreisgüte gering) zu halten, würden sich Verschiebungen dieser Resonanzkurve weniger bemerkbar machen und die Produkte wären vielseitiger verwendbar. Derartige Möglichkeiten liegen in der Erhöhung der Empfindlichkeit der Empfänger der Gate-Antennen und der Transponder-Chips.

Zu den schwer beeinflussbaren Effekten zählt die Umleitung des Magnetflusses und die Wirbelstrombildung in Metallen. Das Wissen darum hilft bei der Planung von Gate-Anlagen und bei der Platzierung von Transpondern an metallhaltigen Medien. Begegnen kann man diesem Effekt nur durch aufwendige Führung des Magnetflusses und in begrenztem Maße durch die Erhöhung der Leistung der Antenne. Der Leistungserhöhung sind allerdings zwei Grenzen gesetzt. Eine Grenze ist eine physikalische. Es lässt sich zwar die Leistung des Senders eines Gates erhöhen um die benötigte Energie den Transpondern zur Verfügung zu stellen. Allerdings wird durch den Effekt im Metall auch die Leistung geschwächt, die vom Transponder beim Empfänger des Gates ankommt. Wenn der Transponder nicht mehr verstanden wird, bringt eine weitere Leistungserhöhung im Gate keinen Effekt. Eine andere Grenze ist der Leistungserhöhung durch die Norm EN300330 gesetzt. Diese Norm geht davon aus, dass ein HF-RFID-Gate keine reguläre Funkanlage ist. Aus diesem Grundgedanken ergibt sich eine starke Beschränkung der abgestrahlten Leistung bei der Arbeitsfrequenz von 13,56 MHz.1

Die hier im Einzelnen betrachteten Effekte zeichnen sich durch die gleiche vom Anwender spürbare Wirkung aus – die Nichterkennung von Transpondern – obwohl sich aus technischer Sicht unterschiedliche Ursachen und Wirkungsmechanismen dahinter verbergen. Durch eine präzise differenzierte Betrachtung kann es in der Praxis gelingen eine Vielzahl von Beeinträchtigungen zu Unterbinden oder zu minimieren und die Funktion von RFID-Systemen angenehmer zu gestalten.

Quelle

[VDI 4478-1] »Testverfahren zur Vereinheitlichung Leistungsbestimmung von RFID-Gates für den Einsatz in Bibliotheken«

1 Nur spezielle Antennenkonstruktionen generieren einen starken Magnetfluss im Erkennungsfeld bei gleichzeitig geringer Störabstrahlung innerhalb des Normwertes.

Hybrid-Automatisierung

Anke Berghaus-Sprengel

Was spricht für den Einsatz von hybriden Automaten?

Eine Umstellung auf RFID gestützte Medienausleihe, Medienrückgabe und Mediensicherung kann in Bibliotheken zumeist nur sukzessive erfolgen, d. h. es ist oft der Fall, dass die traditionelle Ausleihverbuchung und Buchrückgabe mittels Strichcode sowie die Diebstahlsicherung der Medien mit elektromagnetischen Sicherungsstreifen und der Einsatz von RFID gleichzeitig stattfinden müssen.

Ein Grund dafür kann sein, dass die Ausstattung aller Freihandmedien mit Transpondern eine gewisse Zeit benötigt. Ein anderer möglicher Grund in wissenschaftlichen Bibliotheken besteht darin, dass viele Überlegungen dafür sprechen, bestimmte Gruppen von Medien, z. B. nicht ausleihbare Zeitschriftenbände erst gar nicht mit Transpondern auszustatten. Dies auch vor dem Hintergrund, dass aktuell kein Mensch weiß, ob die jetzt verklebten Funketiketten in zehn Jahren noch genauso zuverlässig funktionieren wie heute. Nicht verleihbare Medien müssen nicht ausgeliehen werden können, aber sie sollen auch nicht gestohlen werden.

Man kann sich diverse Logiken des Parallel- oder Hybridbetriebes in der Praxis vorstellen, die jedoch alle ihre Vor- und Nachteile haben. Wenig sinnvoll scheint es beispielsweise zu sein, ein RFID-Sicherungsgate und ein EM-Sicherungsgate im Eingangsbereich hintereinander aufbauen zu wollen.

Um einen Überblick über die verschiedenen Möglichkeiten des Einsatzes von Selbstbedienungskomponenten und Diebstahlsicherungen zu erhalten, ist es notwendig, sich überhaupt erst einmal einen Überblick zu verschaffen, was an Techniken nebeneinander her überhaupt einsetzbar ist bzw. was sinnvoll eingesetzt werden könnte. Erst dann sollte im nächsten Schritt unterschieden werden, ob es sich bei der anzustrebenden Lösung um Parallel- oder um Hybridbetrieb handelt.

Welche Komponenten sind Bestandteile hybrider Automaten?

Um den Praxistest im dritten Abschnitt nachvollziehen und um sich verschiedene hybride Szenarien anschaulich vorstellen zu können ist es sinnvoll, die Funktionsweise und die Einsatzmöglichkeiten der einzelnen beteiligten Komponenten zu unterscheiden:

Barcodes: Auf Etiketten gedruckte Barcodes, die eine eindeutige Mediennummer je gekennzeichnetem Medium enthalten. Oft sind weitere Zusatzinformationen, wie z. B. das Bibliothekssigel integriert. Das Format in Bibliotheken ist häufig 2 aus 5 Interleaved. Damit werden die Länge und das Prüfverfahren festgelegt, durch den ein Barcodereader feststellen kann, ob der Barcode gültig ist. Wird eingesetzt zur Ausleihverbuchung am Tresen oder an Ausleihautomaten. Im Geschäftsgang wird durch Einlesen des Barcodes

der zum Medium gehörende Datensatz im LMS (Library Management System) aufgerufen. Funktioniert nur mit Sichtkontakt zwischen Barcodereader und Barcode.

1. EM-Sicherungsstreifen Kontakt: Sicherungsstreifen, die in die Barcodeetiketten integriert werden, um die Mediensicherung zu ermöglichen. Mit elektromagnetischen Antennen können an Sicherungstoren Alarme erfolgen, sollte ein Medium nicht ausgeliehen sein. Es gibt nur einen Status, ausgeliehen oder nicht. Im Status ausgeliehen ist der Magnetstreifen entmagnetisiert, d. h. unterbrochen, bei nicht ausgeliehen magnetisiert. Auf- und Abwertung können über Magneten oder elektrisch erfolgen, die z. B. in aus Scanner aufgesetzte Manschetten integriert sein können. Die Aktivierung und Deaktivierung erfolgt durch Kontakt des Mediums mit einem Magneten oder durch einen elektronischen Impuls.
2. Tattle Types: Von der Firma 3M entwickelte Sicherungsstreifen. Metallstreifen werden in den Rücken eines Buches geklebt. Funktioniert auch aus Entfernung, sogenannte EM-Distanzsicherung. Keine Integration in Barcode möglich.
3. Transponder: HF-RFID-Etiketten der Frequenz 13,56. Standardetiketten, die im Bibliothekswesen eingesetzt werden. In Deutschland vorwiegend mit Sicherungsbit gemäß ISO 15693/18000-3 Mode 1. Es wird ein sogenanntes AFI-Bit zur Sicherung benutzt. Im Gegensatz dazu z. B. in den skandinavischen Ländern häufig Mediensicherung mit EAS.
4. Transponder UHF: Etiketten im Bereich Ultra High Frequency, d. h. 868 MHZ. Es gibt Pilotversuche im Bibliotheksbereich, vgl. den entsprechenden Artikel im Handbuch. Die große Reichweite bereitet einige Probleme.
5. RFID-Benutzerausweise: RFID-Karten z. B. Mifare Classic, die verschieden eingesetzt werden können. Als klassische Benutzerausweise können sie einfach eine eindeutige Lesernummer enthalten, weitere Daten können selbstverständlich – verschlüsselt oder nicht – je nach Konzept verarbeitet werden.
6. Bezahlkarten: Hier kann es sich um Karten desselben Typs wie unter Punkt 6 beschrieben handeln. Einsatzmöglichkeit als personenunabhängige Guthabenkarte z. B. für die Zahlung von Kopierkosten, Mensaessen, Bibliotheksgebühren, Garderobenschließung etc.
7. Barcode-Benutzerausweise: Ausweise, auf denen ein Barcode aufgedruckt ist, über den sich Leser am Bibliothekssystem anmelden können.

Es gibt nun diverse Möglichkeiten, diese verschiedenen Elemente hybrid oder parallel zu betreiben. Ein Selbstverbuchungsautomat, der z. B. Barcodes einlesen kann und eine Auf- und Abwertung der Mediensicherung mit Tattle-Types vornimmt ist ein Hybridautomat EM-RFID. Genauso kann auch Barcodeverbuchung mit EM-Kontaktsicherung gekoppelt werden. Es wäre dann ebenfalls ein Hybridautomat EM-RFID.

Von einem RFID-Hybridbetrieb würde man sprechen, wenn Medien mit UHF Etiketten genauso verarbeitet werden könnten, wie mit HF-Etiketten. Möglich ist auch der Einsatz von Hybrid-Sicherungsgates, die verschiedene Sicherungssysteme koppeln: EM und HF-RFID oder UHF-RFID und HF-RFID.

Geräte, die Tattle-Types detektieren, lesen in der Regel auch EM-Kontaktsicherungsstreifen, sind darauf aber nicht optimiert.

Praxisbeispiel Hybridbetrieb in der Universitätsbibliothek der Humboldt Universität

Ich werde im Folgenden beispielhaft das an der Universitätsbibliothek der Humboldt Universität zu Berlin eingesetzte Hybridsystem und den dort daneben laufenden Parallelbetrieb an den Mitarbeiterverbuchungsplätzen erläutern.

Die Humboldt Universität hat sich in der Zentralbibliothek im Jacob-und-Wilhelm-Grimm-Zentrum dafür entschieden einen Hybridbetrieb an den Ausleih- und Rückgabeautomaten zu implementieren, die Mediensicherung über ein Hybridtor zu testen und an den Mitarbeiterarbeitsplätzen alternativ Barcodescanner und RFID-Reader im Parallelbetrieb einzusetzen. Alle weiteren Bibliotheksstandorte werden im reinen RFID-Betrieb betrieben.

Es gab zwei Gründe für diese Entscheidung. Zum Einen sollte in einem Praxistest in einer der größten deutschen Universitätsbibliotheken untersucht werden, ob es für wissenschaftliche Bibliotheken Sinn macht, Hybridtechnologie einzuführen. Gerade wissenschaftliche Universalbibliotheken haben in der Regel umfangreiche Bestände, die niemals ausgeliehen werden, die aber gleichwohl dem Leser frei zugänglich aufgestellt sind. Die Umrüstung dieser Bestände wäre sehr teuer, vor allem angesichts der begrenzten Haltbarkeit der Transponder. Die wirtschaftlichste Lösung wäre – bei voller Funktionsfähigkeit – eine Umstellung des Ausleihbestandes auf RFID und eine Beibehaltung der reinen Sicherung des nicht ausleihbaren Bestandes, sei es durch EM-Sicherungsstreifen, sei es durch preiswerte Transponder, die nicht wieder beschrieben werden müssen.

Zum anderen wollte die Bibliothek ein Modell testen, welches es anderen Bibliotheken erlaubt, bei laufendem Betrieb auf RFID umzustellen ohne Schließzeiten oder Perioden nicht gesicherter Medien in Kauf zu nehmen. Auch war es aus zeitlichen Gründen nicht machbar, bis zur Eröffnung des Bibliotheksneubaus im Oktober 2009 alle zwei Millionen Bände, die in Freihand aufgestellt worden sind, rechtzeitig mit Transpondern auszustatten. Das RFID-Projekt hat im Januar 2009 begonnen und ab März 2009 waren die Bücher bereits für den Umzug in Kisten verpackt.

Folgende Techniken wurden seit Oktober 2009 – abwechselnd – eingesetzt:

1. Hybridselbstverbuchungsautomaten an denen Transponder, Barcodes und EM-Sicherungsstreifen verarbeitet werden können.
2. Hybridrückgabeautomaten mit selbiger Leistung.
3. Mitarbeiterarbeitsplätze für den Parallelbetrieb RFID-Reader und Barcodescanner mit Auf-und Abwertungsmanschette für EM-Sicherungsstreifen
4. Hybridsicherungsgate zur Erkennung von EM-Sicherungsstreifen und Transpondern.
5. RFID-Gates zur Mediensicherung

Diese Geräte wurden fast ein Jahr lang eingesetzt und sukzessive optimiert. Folgendes Fazit für den Einsatz von Hybridtechnologie hat die Bibliothek gezogen.

Die Hybridmediensicherung war im Jacob-und-Wilhelm-Grimm-Zentrum nicht einsetzbar. Es war ein sehr großer Eingangsbereich abzusichern, so dass acht Gates gekoppelt

werden mussten. Durch getrennte Antennen sollte immer genau festgestellt werden können, an welchem Tordurchgang das gesicherte Medium durch getragen worden ist. Die Synchronisation dieser Antennen war ein Problem, die Mediensicherung im EM-Bereich wie im RFID-Bereich lag deutlich unter der Erkennungsrate von Toren mit jeweils nur einer dieser beiden Sicherungssysteme. Die Bibliothek hat daher bereits im Dezember 2009 das Hybridtor durch ein reines RFID-Gate ersetzt, welches eine gute Detektion für RFID-gesicherte Medien bietet.

Der Einsatz von Hybridtoren sollte daher genau abgewogen werden. Andere Bibliotheken berichten vom erfolgreichen Einsatz von Hybrid Single oder Double Gates, d. h. von zwei- oder dreischenkligen Hybridtoren. Diese Tore waren bei uns nicht im Einsatz. Im Zweifelsfall sollte hier der Anschaffung eine Testphase vorangehen und die Bibliotheken sollten sich bei den Bibliotheken informieren, die diese Tore einsetzen.

An den Mitarbeiterarbeitsplätzen werden Barcodescanner und RFID-Reader parallel betrieben, d. h. man kann alternativ mit der einen oder der anderen Technik den Barcode ins System einlesen.

Das funktioniert zwar einwandfrei dank der kompletten Einbindung der Software in unser LMS (Library Management System) Aleph 500. Fehleranfällig ist jedoch die Möglichkeit, Mediennummmern alternativ per Handscanner oder per Reader einzulesen. Werden Medien per Barcode verbucht, die einen Transponder besitzen, so wird bei der Ausleihe das sogenannte AFI-Sicherungsbit nicht gesetzt. Das heißt, die Medien sind bei Mitnahmen weiterhin gesichert bzw. werden bei Rückgabe nicht wieder gesichert. Das führt im schlimmsten Fall zu Diebstahl und im lästigen Fall zu Diskussionen mit dem Wachschutz, die jeden aufhalten, der mit einem gesicherten Medium das Haus verlassen möchte. Auf Dauer ist die zusätzliche Ausstattung aller Ausleihplätze mit Reader und Barcodescanner teuer, sinnvoll ist sie für einen Übergangsbetrieb.

Die Hybrid-Selbstverbuchungs- und Rückgabeautomaten sind sicher die heikelsten Lösungen, ist doch ein gewichtiges Argument für die Umstellung auf RFID die Eignung dieser Technik für Selbstbedienungsanwendungen.

Die Auf- und Abwertung der Sicherungssysteme erfolgt an diesen Geräten im Falle des Vorhandenseins eines Transponders durch das Schreiben des AFI-Wertes. Im Falle des Fehlens eines Transponders erfolgt die Auf- und Abwertung durch Magnetisierung bzw. Entmagnetisierung des in den Barcode integrierten Sicherungsstreifens. Bei der Bedienung muss daher darauf geachtet werden, dass der Barcode in einer bestimmten Geschwindigkeit über das Magnetfeld geführt wird.

Die Verbuchung erfolgt durch Einlesen der Mediennummer im Bibliothekssystem. Ist ein Transponder vorhanden, wird dieser durch einen RFID Reader erfasst, ist keiner vorhanden muss der Barcode in einem bestimmten Winkel über einen Barcodescanner geführt werden.

Allein mit Barcode ausgestattete Medien können nicht als Medienpakete verarbeitet werden. RFID-Transponder lassen hingegen die Bündelung mehrerer Teile zu einem Paket ebenso zu, wie die Verbuchung mehrerer Medien gleichzeitig (Stapelverbuchung).

Bei einem Hybridbetrieb muss auf Stapelverarbeitung verzichtet werden, da der Benutzer ja nicht wissen kann, welche Bücher wie ausgestattet sind. Wenn in einem Stapel ein nur mit Barcode befindliches Medium enthalten ist, wird dieses logischerweise nicht erkannt und damit auch nicht verbucht.

Der bei Hybridautomaten genau vorgeschriebene Weg des Buches über den Automaten ist im Hinblick auf die Selbstbedienung natürlich lange nicht so elegant gelöst wie an reinen RFID-Automaten, an denen die Medien erkannt werden, sobald sie in den Bereich eines RFID-Readers kommen.

Die Nutzer sollten daher in den Gebrauch der Automaten intensiv eingewiesen werden. Die Benutzerführung und das Handling der Automaten sollte im Vorfeld genauestens überlegt und ausprobiert werden. Eine allgemein verständliche Benutzerführung und ein durchdachter Menüaufbau ist bei Hybridautomaten noch viel wichtiger als bei reinen RFID-Automaten, bei denen es selbstverständlich auch notwendig ist, im Vorfeld zu überlegen, wie die Bedienung und wie die Dialoge am besten gestaltet werden sollten.

Sind diese Hürden aber genommen, so kann der Hybridbetrieb durchaus sinnvoll sein. In unserem Beispiel konnte die Komplexität der Automaten dadurch gesenkt werden, dass mit Aufgabe der Hybridsicherung die Auf-und Abwertung der EM-Sicherungsstreifen weniger wichtig geworden ist. Es konnte in der Menüführung daher darauf verzichtet werden, das Medium komplett über ein längeres Magnetfeld zu führen. Mit EM-Sicherung hat der Leser immer eine Fehlermeldung erhalten, wenn das Medium zwar ordnungsgemäß verbucht, jedoch noch nicht über den Magneten geführt worden war. Das war für die Leser nicht einsichtig und es wurde häufig der Verbuchungs-Vorgang abgebrochen.

Bisher habe ich nur von Medienausleihe und -rückgabe gesprochen. Der Nutzer muss sich an den Automaten natürlich auch anmelden, um beispielsweise sein Benutzerkonto einsehen zu dürfen, Gebühren zu bezahlen oder eben um ausleihen zu dürfen. Die Nutzeranmeldung erfolgt gängig an Selbstverbuchungsautomaten per RFID-Nutzerkarte und/oder Barcodeleseausweisen. An der Humboldt-Universität ist der Immatrikulationsausweis der Studierenden gleichzeitig der Bibliotheksausweis. Leider konnte der Immatrikulationsausweis aus diversen Gründen noch nicht auf Karte umgestellt werden. Die Universitätsbibliothek hat sich den Aufwand gespart, jedem Nutzer zusätzlich zum Immatrikulationsausweis einen RFID-Leseausweis auszustellen. Auch die universitätsfremden Kunden erhalten zurzeit noch eine Benutzerkarte mit aufgedrucktem Barcode, um einer universitätsweiten Kartenlösung nicht vorzugreifen. Das bedeutet für die Selbstverbuchungsautomaten eine Authentifizierung per Barcode und Passwort. Der Barcode kann über einen Barcodereader eingelesen werden, das Passwort wird per Tastatur eingegeben. Eine Bildschirmtastatur wird aus Datenschutzgründen nicht eingesetzt, alle Automaten besitzen eine vollständige Tastatur zur möglichen Eingabe komplexer Passwörter. Zu Beginn gab es häufiger das Problem, dass z. B. Barcodes auf

Immatrikulationsausweisen, die lange geknickt in Hosentaschen getragen worden sind, schlecht oder gar nicht vom Scanner gelesen werden konnten. Als Konsequenz darf der Leser seine Lesernummer jetzt wahlweise per Scanner oder per Tastatureingabe dem System übermitteln. Man könnte natürlich auch RFID-Ausweise ausgeben und anerkennen lassen, aber es ist schwierig diese möglichen Alternativen dem Menschen am Automaten unmittelbar intuitiv zu vermitteln.

Um die Vielfalt komplett zu machen, haben die Automaten aber zusätzlich einen RFID-Mifare-Kartenleser eingebaut. Dieser dient zur Gebührenannahme. An der Humboldt-Universität besitzen die Studierenden Mensakarten, um damit in der Mensa ihre Speisen oder im Copy-Shop ihre Kopien zahlen zu können. Es handelt sich um reine Guthabenkarten, welche nicht personalisiert sind. Beim Bezahlvorgang wird lediglich eine Gebühr abgebucht und am Automaten eine Quittung generiert.

Fazit

Die Erfahrungen mit dem Einsatz der diversen Erkennungssysteme lassen sich auf einen recht überschaubaren Nenner bringen. Um bei Lesern und Mitarbeitern eine Akzeptanz zu erreichen, sollten Automaten möglichst wenig komplex sein und intuitiv möglichst fehlerfrei bedient werden können. Jede Komplexitätszunahme erfordert eine intensive Beschäftigung mit den Möglichkeiten und Grenzen der hinzukommenden Wahlmöglichkeit. Die Vermittlung dessen, was der Kunde tun soll, tun darf oder nicht tun soll muss gut überlegt werden. Die Auswirkungen und hinzukommenden Fehlerquellen sollten möglichst im Vorfeld genau durchdacht beschrieben werden. Sofern das gelingt, können aber durchaus sinnvoll Zeiten bis zur Umstellung auf nur eine Verarbeitungstechnologie überbrückt werden.

Es sollte aber genau überlegt werden, wie die einzelnen Komponenten zusammenwirken. Die Erfahrung der Bibliothek mit der Hybridsicherung EM-RFID spricht nicht für die Beibehaltung größerer nur mit EM gesicherter Bestände. Diese müssten in einem gesondert gesicherten Bereich stehen.

Die bauliche Situation im Jacob-und-Wilhelm-Grimm-Zentrum mit einem breiten Eingangsbereich und der Möglichkeit gesondert gesicherter Bereich nur im Forschungslesesaal oder in geschlossenen Magazinen bietet diese Option nicht. Insofern ist es für eine Übergangszeit zwar sehr schön, gut funktionierende Hybridausleih- und Hybridrückgabeautomaten einsetzen zu können, aber da ohne funktionierende Sicherung kein Argument für die Nichtsicherung von Medien mit Transpondern spricht, helfen die Automaten nur bedingt.

Würde die Bibliothek noch einmal von vorne beginnen können, würde zweifellos die Entscheidung dahin gehen, alle Medien im Vorfeld mit Transpondern auszustatten und dann auf reine RFID-Automaten umzustellen. Sollte es in absehbarer Zeit gut funktionierende Hybridsicherungssysteme geben oder sollten die baulichen Gegebenheiten die Schaffung andersartig gesicherter Bereiche zulassen, könnte das Ergebnis anders aussehen.

A long way round – Implementierung eines RFID Systems in einer neu gegründeten Bibliothek

Guido Kippelt

Der Einsatz von RFID Technik findet in öffentlichen wie wissenschaftlichen Bibliotheken immer mehr Zuspruch. Die Technik wird verbunden mit effizienteren, zeitsparenden und personalschonenden Arbeitsabläufen im Ausleih- und Rückgabebetrieb. Um die vorhandenen oder geplanten Personalressourcen zu schonen und für andere Dienstleistungen der Bibliothek bereitzuhalten, spricht auf dem ersten Blick alles für die Nutzung dieser Technologie. Im folgenden Artikel soll nun exemplarisch die Planung der Einführung eines RFID Systems am Beispiel der Bibliotheken der Hochschule Hamm-Lippstadt aufgezeigt werden. Es werden die einzelnen Abschnitte und Phasen der Planung bis zum Stand des Prozesses beschrieben. Einführung und Inbetriebnahme sind zum Zeitpunkt der Erstellung dieses Artikels noch nicht abgeschlossen.

Bibliotheken der Hochschule Hamm-Lippstadt

Die Hochschule Hamm-Lippstadt (HSHL) wurde im Jahr 2009 gegründet. Die Schwerpunkte der gelehrten Fachgebiete liegen in den MINT-Fächern. Es sollen an beiden Standorten 5000 Studienplätze entstehen und bis zu 120 Professoren lehren. Im September 2013 sollen laut Bauplan erste Abschnitte der Neubauten, inklusive der Bibliotheken, für die Studierenden geöffnet werden. Die Bibliotheken sind Teil des Zentrums für Wissensmanagement, welches die gesamte Informationsversorgung der Hochschule, die Bereitstellung digitaler Mediendienste und ein breites Angebot an Schulungen zu Fragen der Informationskompetenz, Lern- und Lehrkompetenz sowie Medienkompetenz anbietet. Die Bibliotheken werden an beiden Standorten mit jeweils 3,0 Vollzeitstellen betrieben sowie mit einer Bestandsgröße von ca. 25.000 physischen Medieneinheiten ausgestattet sein. An beiden Standorten sollen RFID Systeme eingerichtet werden.

Gründe/Ursachen für die Entscheidung zur Implementierung von RFID

Die Entscheidung, RFID Technologie in den Bibliotheken der HSHL als Verbuchungssysteme einsetzen zu wollen, basiert auf mehreren Punkten. Ausschlaggebend ist die begrenzte Anzahl an Vollzeitstellen. Deren Einsatzgebiet soll das gesamte Dienstleistungsportfolio der Bibliotheken abdecken. Somit kann hier durch ein funktionierendes RFID System Entlastung in den Arbeitsabläufen der Verbuchung und Rückgabe als auch Arbeitszeit für andere Dienstleistungen generiert werden. Da noch keine organisierten und feststehenden Arbeitsprozesse existieren, ist die Situation einer Neugründung geradezu prädestiniert für die Einführung von RFID Technologie. Es müssen keine etablierten Logistik- und Arbeitsprozesse umgestaltet und den Mitarbeitern neue Abläufe kommuniziert werden. Dieser Themenkomplex ist nicht zu unterschätzen, da in vielen Fällen

eine hohe Nichtakzeptanz und Unsicherheit gegenüber Einführung neuer Systeme beim Personal vorherrschen.

Ein weiterer Grund für die Implementierung von RFID ist die Erstausstattung der Bibliotheken mit Technologien, die zu diesem Zeitpunkt »State of the Art« – Charakter besitzen soll, zu bestücken. Die Bibliothek gewinnt durch ein modernes Verbuchungssystem an Attraktivität für die Nutzer und trägt zur Wahrnehmung der Bibliotheken als Institutionen mit einem modernen Image bei.[1] Aber gerade bei Sichtung des Entwicklungsstands müssen Prioritäten gesetzt werden, da im Detail der angebotenen Systeme Unterschiede vorherrschen. Ein Beispiel hier wäre die Verknüpfung des RFID Systems mit dem jeweiligen Bibliotheks-Management-System (LMS).

Erste Schritte der Umsetzung

Nach dieser Entscheidung folgte eine eingehende inhaltliche Auseinandersetzung, um die technische Funktionsweise eines RFID Systems zu verstehen, sowie eigene detaillierte Anforderungen zu definieren. Diese Anforderungen sollten genau formuliert sein, um bei der späteren Abfrage an die Anbieter eine unmissverständliche Verhandlungsgrundlage vorzuweisen. Weiterhin müssen Voraussetzungen allgemeiner Natur und spezielle Herausforderungen definiert werden.

Eigene Anforderungen, allgemeine Voraussetzungen und spezielle Herausforderungen

Bei der Definition der eigenen Anforderungen muss grundsätzlich geklärt werden, was das RFID System leisten soll und wie bestimmte Arbeitsabläufe innerhalb der Bibliothek geplant werden. Es entstehen Fragen, ob beispielsweise das System primär zum Diebstahlschutz genutzt werden soll. Dann wäre hier das Hauptaugenmerk auf die Verwendung bestimmter leistungsfähiger RFID Tags bei Medienpaketen zu richten. Häufig wird aber der Einsatz der Sicherheitsgates als reine Abschreckungsmaßnahme genutzt und der Erkennung über die Detektionsrate eine eher mindere Rolle zugeschrieben.[2] Ein weiterer möglicher Schwerpunkt wäre sich rein auf die Optimierung des Verbuchungs- und Rückgabevorgang festzulegen, wobei hier die Definition genauer Ablaufszenarien dieser Vorgänge betrachtet werden muss. Letzteres wäre der Fall an den Bibliotheken der HSHL.

Neben den eigenen Anforderungen müssen diverse weitere Faktoren in Betracht gezogen werden, die in vielen Fällen bei erster grober Betrachtung keine Aufmerksamkeit erhalten haben.

Allgemeine Voraussetzungen müssen im Voraus lokalisiert werden. Unter diesen fallen vor allem bauliche Gegebenheiten. Beispiele hierfür sind Lokalisierung von Fluchtwegen und die Beachtung der Barrierefreiheit. Hier muss eine kommunikative Zusammenarbeit

1 Vgl. Keller, Corinne: RFID in Schweizer Bibliotheken – eine Übersicht. Chur, Arbeitsbereich Informationswissenschaft, Bachelorarbeit, 2010, S.28.

2 Vgl. Kern, Christian: RFID in Bibliotheken. Heidelberg: Springer, 2011, S.18.

mit den Planern der Gebäude und im Speziellen mit den Architekten, gerade bei einem Neubau, aufgebaut werden.

In diesem Zusammenhang sollte bei der Planung auf weitere spezielle Herausforderungen eingegangen werden, deren Charakteristik aus der Eigenständigkeit jedes Projekts resultiert. Hier spielen wiederum bauliche Gegebenheiten eine Rolle. Exemplarisch können die vorgesehene Bodenbeschaffung (also Art der Beläge, Einrichtung von benötigten Leerrohren zur Kabelführung usw.) und die Öffnungsrichtung von Türen im Hinblick auf die Positionierung der Sicherheitsgates genannt werden. Aber auch die Beschaffenheit der Türen und der Umgebung der Sicherheitsgates hinsichtlich der Verbauung metallischer Gegenstände, die den Betrieb des elektromagnetischen Wechselfelds zwischen den Gates beeinflussen und stören können, sind zu erwähnen. Hier sollten Abstände von mindestens 0,5 m eingehalten werden.[3] Im Übrigen gilt dies ebenfalls für die Geräte zur Selbstverbuchung für die Nutzer der Bibliothek und die Arbeitsplätze des Personals, an denen RFID Lesegeräte installiert werden sollen. Weiterhin muss die Strom- und Netzwerkversorgung an den neuralgischen Punkten der gewünschten Aufstellung sicher gestellt sein. Solche baulichen Feinspezifika fallen nur bei genauer Betrachtung der Baupläne auf. Wem der Aufbau von und die Symbolik in Bauplänen unbekannt ist, der sollte in jedem Fall beratende Kräfte hinzuziehen, da Planänderungen ab einem gewissen Zeitpunkt im Bauablauf erhebliche Mehrkosten entstehen lassen können.

Eine weitere essentielle Herausforderung ist die Verbindung der einzelnen RFID Komponenten zum LMS. Hier sollte unbedingt darauf geachtet werden, welche Schnittstellen die RFID Systeme der einzelnen Anbieter und das ausgewählte oder vorhandene LMS unterstützt. Zur Auswahl stehen hier die Protokolle SIP2 und NCIP. Wichtig ist hierbei zu ermitteln, welche Anbieter für das entsprechende LMS überhaupt in Frage kommen. Im Fall der Bibliotheken der HSHL handelt es sich um das Open Source Bibliothekssystem koha. Gerade bei so einem, für deutsche Verhältnisse noch »exotischem« LMS sollte explizit bei Anbietern der RFID Systeme nach Referenzen mit diesem System gefragt werden. Die Aufstellung und Durchführung eines Testsystem/-szenario mit den entsprechenden Komponenten in Verbindung mit dem LMS sollte vor der finalen Einrichtung in Erwägung gezogen werden.

Die bisherigen aufgeführten Punkte können weitestgehend bibliotheksintern besprochen werden. Aber gerade bei der Konzeption einer Neugründung von Bibliothek und Hochschule, bei der »auf der grünen Wiese« gestartet wird, sind Diskussionen über das Wie, das Was und das Warum unerlässlich, da in allen Punkten bei Stand null begonnen wird. Es sollte nicht die Sichtweise einer autarken Betriebsorganisation Bibliothek eingenommen werden, da Verflechtungen und Überschneidungen mit der Hochschule in einigen Bereichen unvermeidbar sind. Beispiel hierfür wäre der Einsatz einer hochschulweiten Identifikationskarte. Hier stellen sich Fragen, ob die Karte rein zur Identifizierung genutzt wird, die Integration einer Bezahlfunktion und die Karte an Hochschule und Bibliothek genutzt werden soll. Hier stehen somit verschiedene Modelle zur Wahl. Die

3 Vgl. Seeliger, Frank; Skrobotz, Dieter; Gillert, Frank: Bauliche Aspekte beim Einsatz von RFID. In: Hauke, Petra; Werner, Klaus Ulrich (Hrsg.): Bibliotheken bauen und ausstatten. Bad Honnef: Bock + Herchen, 2009, S.186.

Entscheidung für oder gegen eine dieser Optionen ist eng mit der Hochschulverwaltung abzustimmen, da nachträgliche Änderungen immer einen Mehraufwand bedeuten und durch frühzeitige gemeinsame Planungen vermieden werden können.

Zudem ist mit der Rechtsabteilung der Hochschulverwaltung das Thema Datenschutz und Datensicherheit zu besprechen. Hier ist besonders der Grad der Verschlüsselung der Daten auf den zu nutzenden Karten zu diskutieren. Weiterhin geht es um die Frage, in welchem Umfang und welche Daten der Nutzer auf der Karte gespeichert und ausgelesen werden dürfen, um einen einwandfreien Bibliotheksbetrieb zu gewährleisten. Innerhalb des Themenkomplexes der Benutzeridentifikation wird die Nutzung von Normen eine große Rolle spielen, da hieraus der Grad der Verschlüsselung definiert werden kann. Gerade das Thema Datenschutz ist nicht zu vernachlässigen, da Vorbehalte gegenüber RFID Systemen in der Bevölkerung immer noch vorhanden sind. Da RFID Anwendungsszenarien sich als sehr vielfältig darstellen, ist darauf zu achten, dass die konkrete geplante Ausgestaltung des RFID Systems betrachtet wird.[4]

Ein weiterer Punkt ist die Gebührenbegleichung bzw. Geldtransaktionen der Nutzer zur Bibliothek. Hier ist relevant zu klären, wie der Vorgang der Gebührenzahlung vollzogen werden soll. Es besteht hier die Möglichkeit, Bezahlfunktionen direkt in die Möbel der Selbstverbucher zu integrieren oder aber separate Geräte an anderen Stellen im Bibliotheksraum zu positionieren. Grundsätzlich ist mit der Hochschulverwaltung zu klären ob hier eine RFID Karte eingesetzt wird, die auch Bezahlfunktionen erlaubt. Technisch ist ein solcher Automat über eine SIP2 Schnittstelle mit dem LMS verbunden und benötigt eine Stromversorgung.[5] Bezahlsysteme werden von beinahe allen Anbietern von RFID Anwendungen angeboten.

Zusammenfassend kann festgestellt werden, dass die Definition der eigenen Anforderungen, allgemeinen Voraussetzungen und speziellen Herausforderungen einen zeitlich großen Raum einnehmen und die Ergebnisse eminent bedeutend für alle folgenden Schritte sind, da hier die Basis für das geforderte RFID System der jeweiligen Einrichtung festgelegt wird.

Entscheidungsmatrix, Anforderungskatalog, Leistungsverzeichnis/ Pflichtenheft und Ausschreibung

Die Ergebnisse der im letzten Abschnitt angesprochenen und herausgearbeiteten Anforderungen eines RFID Systems sollten im nächsten Schritt in einen Anforderungskatalog übernommen werden. Dieser Katalog stellt die Basis für eine Entscheidungsmatrix. Nach Erstellung dieser wurden die Anbieter der RFID Systeme zu Terminen eingeladen, um mit ihnen die fixierten Anforderungen zu besprechen. In den meisten Fällen werden die Anforderungen durch die Vertreter der Anbieter bestätigt, was nicht wirklich

4 Vgl. Oltersdorf, Jenny: RFID in Bibliotheken – Ökonomische, juristische und informationsethische Aspekte des Einsatzes von Radio Frequency Identification in Öffentlichen Bibliotheken. Berlin, Magisterarbeit, Institut für Bibliotheks- und Informationswissenschaft, 2007, S.59.

5 Vgl. Kern 2011, S.144.

verwundert. Aus diesem Grund sollte die Recherche über diese Termine hinausgehen. Gerade bei favorisierten Anbietern sollte nach Referenzbibliotheken gefragt werden. Kontakt mit diesen aufzunehmen und Fragen hinsichtlich der Funktions- und Arbeitsweise der genutzten Systeme zu stellen, schafft in vielen Fällen einen hohen Mehrwert zur Einschätzung von Angeboten und möglichen Problemfeldern, die beispielsweise im Zusammenhang mit Hardware oder Support auftreten könnten. Auf Grundlage dieser Erkenntnisse können Anforderungen noch präziser formuliert werden. Dennoch darf nicht unerwähnt bleiben, dass durch eine solche Vorgehensweise, also die Präzisierung, auch unerwartete Ergebnisse bei der späteren Ausschreibung erzeugt werden können und ein Anbieter, der nicht der eigenen Priorität entsprach, das Losverfahren erfolgreich gewinnt. Christian Kern erläutert diese Problematik in seiner Publikation sehr passend.[6]

Trotz dieses Umstandes muss für eine Ausschreibung ein Leistungsverzeichnis/Pflichtenheft verfasst werden. Hier hilft die Angabe von Normen und Richtlinien als festzulegende Referenzen weiter. Es existieren ISO Normen für die Luftschnittstelle der RFID Karten bzw. Etiketten[7], für Datenmodelle[8] sowie eine VDI Richtlinie für Prüfverfahren der Sicherungsgates[9]. Alle anderen Kriterien müssen über Ausschlusskriterien oder Beschreibungen selbst generiert werden.[10] Beide Verfahren bergen Vor- und Nachteile und es kann somit keine Präferenz ausgesprochen werden.

Abschließende Empfehlungen

Ziel dieses Artikels war es, den komplexen Prozess der Anschaffung eines RFID Systems an einer neugegründeten Bibliothek in seinen möglichen Facetten aus Anwendersicht darzustellen. Alle Facetten und Problembereiche darzustellen, hätte die Grenzen eines Artikels übersteigen. Hieraus folgt die Erkenntnis, dass es sich um einen komplexen Sachverhalt handelt. Wenn eine Bibliothek die Anschaffung eines RFID Systems in Erwägung zieht, ist eine frühzeitige Auseinandersetzung mit dieser Technologie absolut zu empfehlen. Hier ist die einschlägige Fachliteratur zu verwenden. Aber auch die Recherche in anderen Bibliotheken stellt einen großen Nutzen für den weiteren Entscheidungsprozess dar. Das erworbene Wissen dient als gute Basis für Gespräche mit Anbietern, aber natürlich im Besonderen bei der Gestaltung von Anforderungskatalog, Leistungsverzeichnis und Ausschreibung.

Das erworbene Wissen spielt zudem eine Rolle bei der Gebäudeplanung mit Architekten und den ausführenden Parteien. Hier sind die aufgezeigten Sachverhalte in aller Tiefe zu diskutieren. Abschließend sind die Abstimmungen mit Teilen der Hochschule im Hinblick auf die Themenfelder Benutzeridentifikation über eine Hochschulkarte und Datenschutz zu beachten.

---

6 Vgl. Kern 2011, S.115-116.
7 ISO 15693 und ISO 18000-3.1
8 ISO 28560-1, -2 und -3
9 VDI 4478-1
10 Vgl. Kern 2011, S.116-117.

Literatur und Internetquellen

[1] Keller, Corinne: RFID in Schweizer Bibliotheken – eine Übersicht. Chur, Arbeitsbereich Informationswissenschaft, Bachelorarbeit, 2010.

[2] (KERN 2011) Kern, Christian: RFID in Bibliotheken. Heidelberg: Springer, 2011.

[3] Oltersdorf, Jenny: RFID in Bibliotheken – Ökonomische, juristische und informationsethische Aspekte des Einsatzes von Radio Frequency Identification in Öffentlichen Bibliotheken. Berlin, Magisterarbeit, Institut für Bibliotheks- und Informationswissenschaft, 2007.

[4] Seeliger, Frank; Skrobotz, Dieter; Gillert, Frank: Bauliche Aspekte beim Einsatz von RFID. In: Hauke, Petra; Werner, Klaus Ulrich (Hrsg.): Bibliotheken bauen und ausstatten. Bad Honnef: Bock + Herchen, 2009.

RFID bei der Fernleihe

Cathrin Neumair

Die Einführung des Dänischen Datenmodells stellt einen wichtigen Meilenstein in Richtung Vollautomatisierung der Fernleihe im Bibliothekswesen dar. Obwohl dieses Modell in immer mehr Bibliotheken eingeführt wurde, vollzieht sich die Abwicklung der Fernleihe in der Praxis vorwiegend teilautomatisiert. Der vorliegende Artikel liefert eine Bestandsaufnahme der gegenwärtigen Teilautomatisierung in der Fernleihe und zeigt neue Lösungsansätze auf, wie eine Vollautomatisierung in der Zukunft aussehen kann.

1. Allgemeines zur Fernleihe

Im Rahmen der Fernleihe kann eine Bibliothek ihren Benutzern Literatur (Bücher und Aufsatzkopien) zur Verfügung stellen, die am Ort nicht vorhanden ist. Diese Dienstleistung ist bei manchen Bibliotheken für den Benutzer kostenpflichtig, und es wird eine Pauschalgebühr ab 1,50 Euro pro Bestellung erhoben [1].

Im Allgemeinen wird bei der Fernleihe zwischen der aktiven und passiven Fernleihe unterschieden.

Bei der aktiven Fernleihe (AFL), auch gebende Fernleihe genannt, werden Bücher aus der eigenen Bibliothek an fremde Bibliotheken verliehen, damit diese sie ihren eigenen Benutzern zur Verfügung stellen können.

Werden dagegen Bücher für die eigenen Benutzer aus fremden Bibliotheken ausgeliehen, handelt es sich um eine passive bzw. nehmende Fernleihe (PFL).

Geregelt wird die Fernleihe in der Leihverkehrsordnung (LVO) [2]. Hier sind die Bedingungen, Regeln und Bestimmungen, die für den Leihverkehr zwischen den Bibliotheken in der Bundesrepublik Deutschland gelten, im Einzelnen beschrieben. Auf einige Inhalte soll an dieser Stelle kurz eingegangen werden.

Die zwei wichtigsten Grundsätze in der Leihverkehrsordnung sind das Regionalprinzip und das Prinzip der Gegenseitigkeit [3].

Das Regionalprinzip

Jede Bibliothek hat die Pflicht, zunächst zu prüfen, ob das Medium im eigenen Bestand oder bei einer anderen öffentlichen Bibliothek vor Ort vorhanden ist. Ist dies nicht der Fall, wird die Bestellung auf die eigene Leihverkehrsregion (den Verbundkatalog, z. B. Gateway Bayern) ausgeweitet. Sollte eine Bestellung bei der eigenen Leihverkehrsregion nicht möglich sein, kann die Bestellung an andere Regionen weitergeleitet werden.

Das Prinzip der Gegenseitigkeit

Eine Bibliothek kann an der Fernleihe teilnehmen, wenn sie nicht nur Medien über die Fernleihe ausleiht (nehmend), sondern sich auch verpflichtet, ihren eigenen Bestand für die Fernleihe zur Verfügung zu stellen (gebend).

Daneben ist in der Leihverkehrsordnung festgelegt, dass nicht jede Literatur über die Fernleihe bestellt werden kann. Da die Fernleihe bzw. der Leihverkehr primär die Forschung und Lehre sowie die Aus-, Fort-und Weiterbildung sowie die berufliche Tätigkeit unterstützen soll, sind z. B. Unterhaltungsromane, Sachbücher (z. B. Kochbücher), Reiseführer usw. ausgeschlossen. Diese werden für gewöhnlich bei einer anderen öffentlichen Bibliothek am Ort angeboten oder sind im Handel zu einem relativ geringen Preis (unter 15 Euro) erhältlich. Auch Loseblattsammlungen, AV-Materialien, CDs, DVDs, Hörbücher und nicht zuletzt alte oder sehr wertvolle Bücher (Verlustrisiko) oder großformatige Bücher wie z. B. Bildbände (Versandproblem) können in der Regel nicht über die Fernleihe bezogen werden.

Der Ablauf der Fernleihe gestaltet sich wie folgt. Besitzt ein Bibliotheksbesucher einen Bibliotheksausweis, kann er nach Eingabe von Benutzernummer und Passwort über den Bibliothekskatalog (OPAC) der Heimatbibliothek (falls eine Schnittstelle zum Verbundkatalog vorhanden ist) oder aber auch direkt über den Verbundkatalog eine Online-Fernleihe anstoßen.

Gibt es die Möglichkeit der direkten Online-Fernleihbestellung für den Bibliotheksbesucher nicht, muss er sich an einen Mitarbeiter seiner Bibliothek wenden. Dieser übernimmt die notwendigen Recherchearbeiten und leitet die Bestellung weiter.

Die Ausleihbedingungen wie Leihfristen, Ausleihe außer Haus oder nur in den Räumen der Bibliothek u. a. m. legt im Allgemeinen die Bibliothek fest, der das bestellte Medium gehört [4].

2. Fernleihe und RFID

Immer mehr Bibliotheken nutzen statt Barcode und EM-Streifen (zur Sicherung des Mediums) die Möglichkeiten von RFID. Sie bieten dem Bibliotheksbenutzer innerhalb der Bibliothek ein eigenständiges, schnelles und komfortables Verbuchen der Medien an Selbstverbuchungsanlagen und Rückgabeautomaten. Es können mehrere Medien in einem Vorgang gelesen und verbucht werden (Stapelverbuchung). Voraussetzung hierfür ist, dass der gesamte Bestand mit RFID-Tags versehen ist.

Nun steht die Frage im Raum, wie man die Fernleihe mit RFID verbinden kann bzw. inwiefern RFID allgemein für die Abwicklung der Fernleihe von Nutzen sein kann.

2.1 Passive Fernleihe

In der Regel wird die Fernleihbestellung eines Fernleihbuches sofort auf das Konto des Benutzers im Bibliothekssystem verbucht. Meistens ist eine Schnittstelle zwischen dem Fernleihserver auf Verbundebene und den lokalen Bibliothekssystemen vorhanden. Während der Bestellung wird eine so genannte Fernleihnummer (PFL-Nummer) generiert, mit der alle nachstehenden Verbuchungen wie die Eingangsverbuchung, die Ausleih- und Rückgabeverbuchung an und vom Benutzer und auch der Rückversand an die gebende Bibliothek durchgeführt werden.

Bevor RFID im Bibliotheksbereich zum Einsatz kam, wurden Fernleihmedien anhand der Fernleihnummer entweder manuell oder, sofern der Fernleihschein mit einem Barcode mit PFL-Nummer ausgestattet war, mit einem Barcode-Scanner verbucht.

Da der Einsatz von RFID ein selbständiges Verbuchen an den SB-Terminals ermöglichen soll, muss überlegt werden, wie die passive Fernleihe an den SB-Terminals eingebunden werden kann. Darüber hinaus sollte RFID bei Fernleihmedien auch an der Ausleihtheke einsetzbar sein.

Nachfolgend werden diverse teilautomatisierte Möglichkeiten einer Umsetzung der RFID-Technologie für die Fernleihe dargestellt.

2.1.1 Fernleihmedium mit Barcode-Etikett (ohne RFID-Label)

Wenn das Fernleihbuch nicht mit einem RFID-Label ausgestattet ist, besitzt es dennoch ein Barcode-Etikett mit der Mediennummer der gebenden Bibliothek. Um ein solches Medium „RFID-fähig“ zu machen, muss die nehmende Bibliothek ein RFID-Label mit der entsprechenden PFL-Nummer beschreiben und in das Medium einbringen.

In diesem Zusammenhang nutzen einige Bibliotheken die folgenden praxiserprobten Lösungen:

Wird das Fernleihmedium von der gebenden Bibliothek geliefert, muss dessen Eingang zunächst manuell verbucht werden. Dabei wird der Fernleihzettel in eine Klarsichthülle (DIN A6) gelegt. Die Hülle wird anschließend mit einem RFID-Label beklebt, das mit der Fernleihnummer beschrieben wurde. Die Hülle wird nun mit dem Fernleihzettel in das Buch gelegt. Auf diese Weise kann das Fernleihmedium über die Selbstverbuchung verbucht und über den Buchrückgabeautomaten zurückgegeben werden.

Nach Rückgabe des Fernleihbuches werden die Daten auf dem Label gelöscht, so dass es wieder neu verwendet werden kann [5].

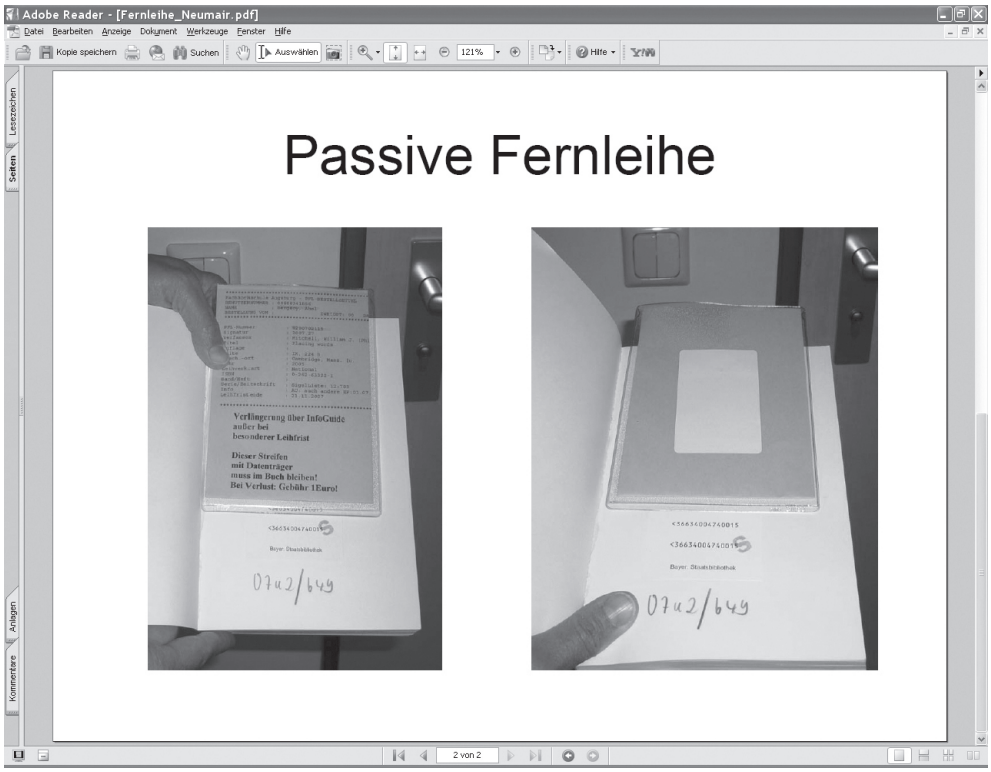


Abb. 1: Fernleihzettel in einer Hülle mit RFID-Etikett, ©HB Augsburg

Andere Hochschulbibliotheken kleben das RFID-Label nicht auf eine Hülle, sondern direkt in das Fernleihmedium. Dies erlaubt, das Label nach der Rückgabe wieder problemlos aus dem Fernleihmedium zu entfernen [6].

Bei diesen Lösungen kann es vorkommen, dass das RFID-Label verloren geht. Dann ist aber auch keine Verbuchung an den Automaten mehr möglich.

2.1.2 Fernleihmedium mit RFID-Label

Besitzt das gewünschte Medium bereits ein RFID-Label der gebenden Bibliothek, kann es im Allgemeinen vom RFID-Reader der nehmenden Bibliothek gelesen und auch beschrieben werden.

Es gibt jedoch Fälle, bei denen ein automatisiertes Einlesen des RFID-Transponders nicht funktioniert.

Verschiedene RFID-Tags/Chips

Auf dem Markt werden verschiedene RFID-Tags bzw. Etiketten angeboten. Diese besitzen zum Teil unterschiedliche Chips mit unterschiedlichen Speicherkapazitäten und -strukturen. Hier kann es vorkommen, dass manche Chips vom eigenen Reader bzw. von der Software nicht gelesen werden können. Als Beispiel wäre der Light-Chip zu nennen.

Dieser besitzt nur eine Speicherkapazität von 256 Bit und kann momentan noch nicht von allen RFID-Geräten gelesen werden [7].

Unterschiedliche Datenmodelle

Seit ca. 2005 existiert das Dänische Datenmodell. Es wurde eingeführt, um die Komponenten der RFID-Systeme verschiedener Hersteller miteinander kompatibel zu machen. Das Dänische Datenmodell definiert die erforderlichen Elemente (Mediennummer, ISIL, mehrteilig (ja/nein)), die Anzahl der Teile und den Status (Sicherung aktiv/inaktiv (AFI-Paar)) und legt deren Positionen und Länge auf dem Chips fest. Daher sind RFID-Tags von Bibliotheken, die RFID vor Einführung des Dänischen Datenmodells implementiert haben, nicht mit dem Dänischen Datenmodell kompatibel. Die Informationen können vom RFID-Gerät nicht gelesen werden. Dies ist auch bei einigen ausländischen Bibliotheken mit anderen, individuellen Lösungen der Fall [8].

Abweichende AFI-Werte

Das Sichern und Entsichern des Mediums wird über das so genannte AFI-Paar geregelt. Es ist fester Bestandteil des Dänischen Datenmodells. Seit August 2008 gilt für Medien außerhalb der Bibliotheken der AFI-Wert C2 (entsichert), für Medien innerhalb der Bibliotheken der Wert 07 (gesichert). Einige Bibliotheken arbeiten jedoch mit anderen Werten (z. B. 92/91 gemäß Dänischem Entwurf bis Juli 2005 oder 9E/9D im Rahmen des Dänischen Modells ab Juli 2005). Diese Abweichungen der AFI-Paare führen dazu, dass die Information vom RFID-Reader zwar gelesen werden kann, die Funktion des Sicherns und Entsicherns aber nicht funktioniert, d. h. das am Gate kein Alarm ausgelöst wird [9].

Kann das RFID-Label der gebenden Bibliothek aufgrund des RFID-Tags oder unterschiedlicher Datenmodelle vom eigenen Reader nicht gelesen werden, kann die nehmende Bibliothek alternativ wie bei einem Barcode-Etikett verfahren und ein zusätzliches RFID-Etikett mit eigener PFL-Nummer verwenden.

Wenn der Reader das RFID-Etikett der fremden Bibliothek lesen kann, kann es für die Verbuchung trotzdem nicht herangezogen werden. Grund hierfür ist die Mediennummer der fremden Bibliothek, die im eigenen Bibliotheksystem nicht existiert. Deshalb muss wieder ein zweites Label mit der eigenen PFL-Nummer in das Medium integriert werden. Beim Verbuchen an der Ausleihtheke (s. Abbildung 2: Stapelverbuchung im Ausleih-Client) oder am SB-Terminal werden aber beide Labels angezeigt:

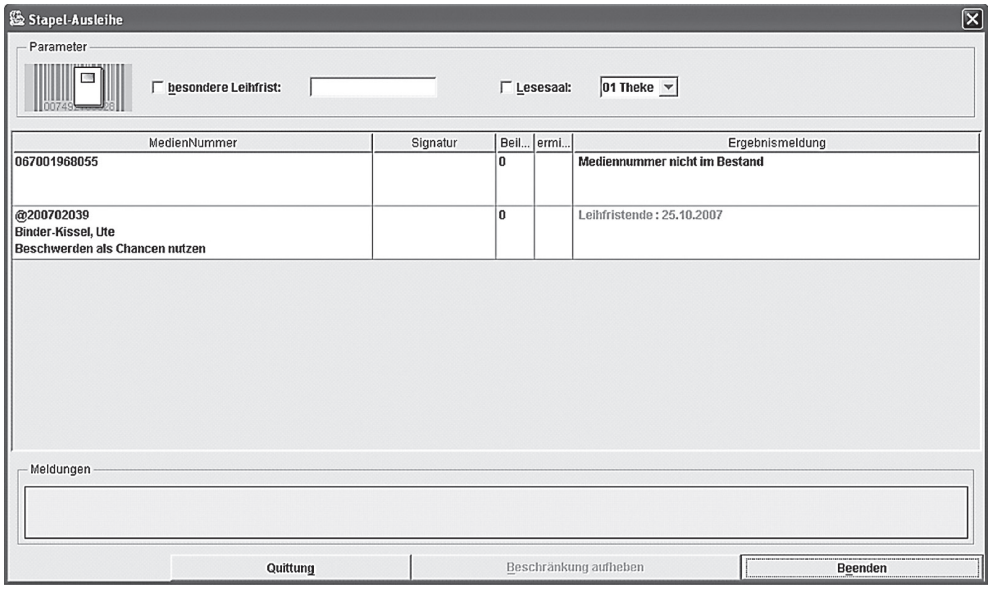


Abb. 2: Stapelverbuchung im Ausleih-Client, © Fa. OCLC

Beim fremden Label wird allerdings darauf hingewiesen, dass dieses Medium nicht im Bestand der eigenen Bibliothek ist, was für den Benutzer beim Verbuchen des Fernleihmediums am SB-Terminal etwas irritierend sein kann.

Außerdem kann diese Lösung nicht bei Rückgabeautomaten eingesetzt werden. An dieser Stelle ist nur Einzelverbuchung möglich. Da die beiden Labels des Mediums nicht gleichzeitig gelesen werden können, wird es vom Automaten zurückgewiesen.

Dieses Problem kann vermieden werden, indem die Software des Automaten so angepasst wird, dass nur die PFL-Nummer an das Bibliotheksystem übergeben wird. Als Prüfkriterium kann das internationale Sigel ISIL (International Standard Identifier for Libraries and Related Organizations) verwendet werden. Es werden zwar beide RFID-Labels gelesen, aber nur die Mediennummer mit dem eigenen Sigel wird an das Bibliothekssystem weitergeleitet [10]. Zu beachten ist allerdings, dass der Automat nicht erkennen kann, ob nun zwei Medien mit jeweils einem RFID-Label oder ein Medium mit zwei RFID-Labels zurückgegeben werden.

Um zu verhindern, dass ein Alarm ausgelöst wird, wenn der Benutzer die Bibliothek mit dem Medium verlässt, sollte geprüft werden, ob das fremde RFID-Label entsichert werden muss. Ist das AFI-Paar nicht identisch, ist eine Entsicherung des Labels nicht erforderlich. Falls aber das fremde RFID-Label das gleiche AFI-Paar benutzt und dieses den Status „Sichern“ besitzt, muss es auf „Entsichern“ gesetzt werden. Hier wäre es sinnvoll, bereits bei der Eingangsverbuchung zu überprüfen, in welchem Status sich das Label befindet. Nach dem Entsichern kann das zweite RFID-Etikett ins Buch eingebunden werden.

Die oben beschriebenen Lösungen stellen jedoch nur Behelfslösungen dar. Da RFID zunehmend in Bibliotheken eingesetzt wird, muss eine umfassende Lösung gefunden werden. In Abschnitt 3 werden mögliche Lösungen zur Verbuchung mit RFID-Label der gebenden Bibliothek erläutert.

2.1.3 Ausgabeort

Die Fernleihmedien liegen in der Regel im Abholregal bereit und werden von dort eigenständig abgeholt und am SB-Terminal verbucht. Mancherorts können sie auch nur über die Ausleihtheke abgeholt werden. Eine weitere Möglichkeit stellt der Einsatz von einem Fernleihautomaten dar. Dieser besitzt verschiedene Schubladen, in denen sich die Fernleihmedien befinden. Der Benutzer gelangt zu seinem Buch, indem er sich am Automaten zuerst mit seiner Kennung anmeldet und in der Titelliste das gewünschte Buch auswählt. Mittels Anweisung auf dem Bildschirm wird er anschließend dazu aufgefordert, das Buch aus Schublade »*XY*« zu entnehmen. Nachdem er das Medium aus der Schublade entnommen und die Schublade geschlossen hat, wird das Fernleihmedium automatisch über das Bibliothekssystem ausleihverbucht. Die Rückgabe geschieht über den RFID-Rückgabeautomaten, da sich im Buch ein entsichertes RFID-Label mit der PFL-Nummer befindet [11].

2.2 Aktive Fernleihe

Immer mehr Bibliotheken, die aktive Fernleihe betreiben, haben RFID im Betrieb und speichern ihre Daten gemäß dem Dänischen Datenmodell. Deswegen sollten sie als gebende Bibliothek das Label entsichern („Medium außer Haus“), wenn sie das Buch in den Leihverkehr geben. So kann verhindert werden, dass am Gate der nehmenden Bibliothek Alarm ausgelöst wird, da die nehmende Bibliothek nicht immer die Möglichkeit hat, die Sicherung mit der eigenen Software zu deaktivieren. Die einfachste Vorgehensweise ist deshalb, dass die gebende Bibliothek die Sicherung bei der Ausgangsverbuchung deaktiviert und sie bei der Rückgabe wieder aktiviert.

3. Zusammenfassung

Bei näherer Betrachtung der oben beschriebenen Varianten zur Umsetzung von RFID in der Fernleihe fällt auf, dass der zeitliche und organisatorische Aufwand bei allen Möglichkeiten sehr ähnlich ist, da immer ein RFID-Label erstellt werden muss. Der Vorteil des Dänischen Datenmodells zur Standardisierung der Daten kommt nicht wie gewünscht und erwartet zur Geltung. Einer Vollautomatisierung steht das manuelle Erstellen eines Labels im Weg. Mittelfristig wird jedoch sicherlich eine Entwicklung zur Vollautomatisierung stattfinden, bei der auch die nehmende Bibliothek das Originallabel verwendet. Hier gibt es verschiedene Lösungsansätze.

Nachfolgend sollen zwei Möglichkeiten skizziert werden, wie eine Vollautomatisierung in der Praxis aussehen könnte. Beide Varianten setzen dabei das Dänische Datenmodell voraus [12].

3.1 Konkordanz zwischen Originalmediennummer und PFL-Nummer

Bei dieser Lösung gibt es innerhalb des Bibliothekssystems eine Verknüpfung zwischen der Originalmediennummer und der PFL-Nummer. Dies geschieht dadurch, dass zusätzlich zur PFL-Nummer die Originalmediennummer im Bibliotheksystem hinterlegt wird und beide eindeutig miteinander verknüpft werden.

Der Prozess läuft folgendermaßen ab: Das entsicherte Fernleihbuch wird von der gebenden Bibliothek geliefert. Die nehmende Bibliothek sichert das Medium gemäß ihren AFI-Werten, da womöglich nicht dasselbe AFI-Paar verwendet wurde, und führt die Eingangsverbuchung durch. Bei diesem Vorgang wird auch die Originalmediennummer in das Bibliothekssystem übertragen. Nachdem nun die Originalmediennummer im Lokalsystem der nehmenden Bibliothek registriert wurde, funktioniert auch die Verbuchung am SB-Terminal bzw. Rückgabeautomat.

Um jedoch eine absolute Eindeutigkeit des (Fernleih-)Mediums zu gewährleisten, wäre es sinnvoll, neben der Originalmediennummer auch das ISIL als zusätzliches Prüfkriterium zu ergänzen. Es ist durchaus denkbar, dass dieselbe Mediennummer sowohl im lokalen Bestand der nehmenden Bibliothek als auch in einer oder mehreren gebenden Bibliotheken verwendet wird.

Bevor das Fernleihmedium wieder an die gebende Bibliothek zurückgesendet wird, wird die Verknüpfung zwischen Mediennummer des Originallabels und der PFL-Nummer aufgelöst und die Sicherung deaktiviert.

3.2 Zusätzliche Speicherung der PFL-Nummer auf dem RFID-Tag

Ein weiterer Lösungsansatz zielt darauf ab, die PFL-Nummer in das Originallabel zu integrieren. Das Dänische Datenmodell besitzt neben den Pflichtelementen optionale Felder, die frei belegt werden können. Dort kann die PFL-Nummer eingetragen werden.

Der Prozess geht folgendermaßen vonstatten: Bei der Eingangsverbuchung wird die PFL-Nummer mit Hilfe einer RFID-Software in einem optionalen Feld des Labels gespeichert und die Sicherung mit den eigenen AFI-Werten wieder aktiviert. Aus Gründen der Datensicherheit sollten nur diese beiden Felder beschreibbar sein.

Beide Felder können von den Automaten gelesen werden. Es muss jedoch noch geprüft werden, welches der beiden Felder in das Bibliothekssystem übergeben werden soll. Dies kann wiederum über das ISIL erfolgen, oder es wird abgefragt, ob das PFL-Feld belegt ist. Beim Rückversand wird die PFL-Nummer am RFID-Label wieder gelöscht und die Sicherung deaktiviert.

4. Ausblick

Bei den genannten Lösungsvorschlägen sind allerdings an den Automaten, im Bibliothekssystem und am Ausleih-Client Softwareänderungen erforderlich, wodurch zusätzliche Kosten entstehen. Welche Lösung sich letztendlich in der Praxis mit dem geringsten Aufwand implementieren lässt, kann zum jetzigen Zeitpunkt noch nicht abschließend beurteilt werden. Hier besteht sicherlich noch Diskussionsbedarf. Angesichts der zunehmenden Verbreitung von RFID im Bibliothekswesen sollte jedoch eine zeitnahe Umsetzung angestrebt werden.

Literatur und Internetquellen

[1] Wikipedia (2009) Fernleihe http://de.wikipedia.org/wiki/Fernleihe

[2] Die Ordnung des Leihverkehrs in der Bundesrepublik Deutschland (2003/2004), http://www.bibliothek.uni-regensburg.de/pdf/lvo.pdf

[3] Wikipedia (2010) Leihverkehrsordnung http://de.wikipedia.org/wiki/Leihverkehrsordnung

[4] Wikipedia (2009) Fernleihe http://de.wikipedia.org/wiki/Fernleihe

[5] Angelika Hofmockel (2008) Service-Erweiterung mit RFID an der Fachhochschulbibliothek Augsburg (S. 31-32), http://www.th-wildau.de/fileadmin/dokumente/bibliothek/dokumente/Vortrag_Wildau_2008_Service-Erweiterung_Hofmocke_V2.pdf

[6] Uwe Dierolf (2009) RFID-Fernleihe (UB Karlsruhe (S. 6)), http://blog.ubka.uni-karlsruhe.de/aspb/wp-content/uploads/2009/05/dierolf_vortrag_aspb_rfid_fernleihe.pdf

[7] 2. Treffen der RFID-Anwendergruppe in Mannheim am 2. Juni 2008 http://www.bibliotheksportal.de/hauptmenue/themen/rfid-in-bibliotheken/ag-rfid-in-bibliotheken/

[8] RFID Data Model for Libraries (2005) (S. 22), http://biblstandard.dk/rfid/dk/RFID_Data_Model_for_Libraries_July_2005.pdf

[9] Wolfgang Friedrich (2008) RFID Normung (RFID Tag Datenmodelle – internationale und nationale Standardisierungsansätze) (S. 23), http://www.bibliotheksportal.de/hauptmenue/themen/rfid-in-bibliotheken/normierung/

[10] Uwe Dierolf (2009) RFID-Fernleihe (UB Karlsruhe (S. 46)), http://blog.ubka.uni-karlsruhe.de/aspb/wp-content/uploads/2009/05/dierolf_vortrag_aspb_rfid_fernleihe.pdf

[11] Uwe Dierolf (2009) RFID-Fernleihe (UB Karlsruhe), http://blog.ubka.uni-karlsruhe.de/aspb/wp-content/uploads/2009/05/dierolf_vortrag_aspb_rfid_fernleihe.pdf

[12] Robert Scheuerl (2009) RFID in den Verbundbibliotheken (S. 22), http://www.bib-bvb.de/vk2009/scheuerl_bvbvk2009.pdf

Die zitierten Internetquellen wurden zuletzt am 31.05.2010 aufgerufen.

Einflüsse von NFC-Smartphones auf das RFID-Bibliothekssystem

Eine Analyse des Bedrohungspotentials durch NFC-Smartphones und Beschreibung von möglichen Gegenmaßnahmen

Sebastian Krautz

Dieses Kapitel soll einen Einstieg in die Problematik von NFC-Einflüssen auf Bibliothekssysteme geben. Dazu werden die Eigenschaften der beteiligten Systemkomponenten kurz erklärt. Anschließend werden zwei Hauptangriffsszenarien mit den Auswirkungen für eine Bibliothek beschrieben. Des Weiteren werden mögliche Wege aufgezeigt, wie solche Angriffe verhindert werden können und was bei Einsatz solcher Lösungen beachtet werden muss.

Einleitung

RFID wird in Bibliotheken mittlerweile seit vielen Jahren erfolgreich eingesetzt. Die Technologie wird dabei sowohl zur Unterstützung von Prozessen innerhalb der Bibliothek, wie etwa der Ausleihe eines Buches, als auch zur Diebstahlsicherung genutzt. In den letzten Jahren hat sich dieses System bewährt und ist aus einer modernen Bibliothek nicht mehr wegzudenken. Dieses System steht nun jedoch vor einer Herausforderung.

In Asien bereits sehr weit verbreitet, setzt sich auch bei uns eine neue Technologie, die sogenannte Near Field Communication (NFC), immer mehr durch. Diese Technologie wird vor allem in neuen Smartphones[1] eingesetzt. Sie basiert im Grunde auf RFID. Damit stellt NFC quasi einen kleinen RFID-Reader für jedermann zur Verfügung. Warum stellt dieser Fakt nun eine Herausforderung für das RFID-Bibliothekssystem dar!? Es ist deshalb eine Herausforderung, da nun »jeder« mit entsprechenden Mitteln relativ einfach beispielsweise die zur Diebstahlsicherung verwendeten Parameter mit seinem Smartphone verändern und somit außer Kraft setzen kann.

Aber auch weitere Angriffspunkte sind durch die Verwendung von NFC gegeben. Welche dies genau sind und welche Ansätze es gibt, um diesen zu begegnen wird im weiteren Verlauf noch genauer beleuchtet.

1 Smartphone: nach Definition ein Mobiltelefon, welches einen leistungsstarken Prozessor besitzt und zusätzliche Geräte, wie Kameras, MP3-Player und Navigationssysteme enthält. [vgl. eteleon.de]

Ausgangssituation

Die Verbreitung von NFC-fähigen Smartphones sorgt bei vielen Bibliothekaren und Bibliotheksmitarbeitern für erhebliche Bedenken hinsichtlich der Einflüsse und Möglichkeiten der neuen Technologie im Bibliotheksumfeld. Daher wurde diese Thematik im Rahmen einer Masterarbeit näher untersucht. Die folgenden Abschnitte sollen kurz die nötigen Hintergrundinformationen zu Technologie, Standards und beteiligten Komponenten liefern.

NFC-Technologie

Die Technologie entstand bereits 2002. Sie basiert auf der Funktionsweise von induktiven RFID-Systemen. Die benutzte Frequenz liegt im, von den Bibliotheken häufig verwendeten, HF-Bereich bei 13,56MHz. Damit können Datenraten bis zu 424 kbit/s erreicht werden [vgl. 1]. Die Technologie basiert also ebenfalls auf der Erzeugung magnetischer Felder. Diese werden über eine Erzeugerspule aufgebaut. Eine solche Spule ist in der Regel in den entsprechenden NFC-Smartphones enthalten. Die Gegenstelle bildet auch hier ein Transponder. Das besondere bei NFC ist jedoch, dass die Gegenstelle kein normaler Transponder sein muss, sondern es kann ebenfalls ein weiteres NFC-Smartphone sein. Das wird durch einen besonderen Modus bei NFC ermöglicht, der bei herkömmlichen RFID-Systemen nicht zur Verfügung steht.

Für die Technologie gibt es zwei zentrale Standards. Den ersten bildet das Near Field Communication Interface and Protocol 1 (NFCIP-1). Hinter diesem steht der ISO Standard 18092. In diesem Standard werden die Übertragungsprotokolle von MIFARE und FeliCa kombiniert. Außerdem werden diese darin um zusätzliche Kommunikationsmöglichkeiten erweitert. Als letztes Merkmal wird ein neues Transportprotokoll ergänzt. Durch diesen Standard werden drei Übertragungsgeschwindigkeiten definiert, die auf den enthaltenen Protokollen basieren. So werden 106kbit/s auf Basis von MIFARE und 212kbit/s und 424kbit/s auf der Basis von FeliCa vorgeschrieben. [vgl. 1]

Der zweite Grundstandard für NFC ist NFCIP-2 mit dem zugehörigen ISO Standard 21481. In diesem werden die Funktionalitäten verschiedener Systeme zusammengeführt. Dazu zählen Proximity[2]- und Vicinity[3]-Systeme. Zu den Vertretern der Proximity zählen ISO 14443A und ISO 14443B. Zu den Vicinity gehört ISO 15693. Geräte die auf dem ISO 21481 Standard basieren, können also in diesen drei Bereichen operieren. Dazu wird definiert, wie dabei die Auswahl eines der drei möglichen Modi zu treffen ist. Wie NFCIP-1 und NFCIP-2 in die NFC-Landschaft einzuordnen sind, ist in der nächsten Abbildung dargestellt.

2 Proximity: bezeichnet Systeme mit einer Reichweite bis zu zehn Zentimeter. Ein Reader wird dabei als Proximity Coupling Device(PCD) und ein Transponder als Proximity Integrateted Circuit Card (PICC) bezeichnet.

3 Vicinity: bezeichnet Systeme mit einer Reichweit bis zu 50 oder auch 100 Zentimetern. Ein Reader wird dabei als Vicinity Coupling Device(VCD) und ein Transponder als Vicinity Integrated Circuit Card(VICC) bezeichnet.

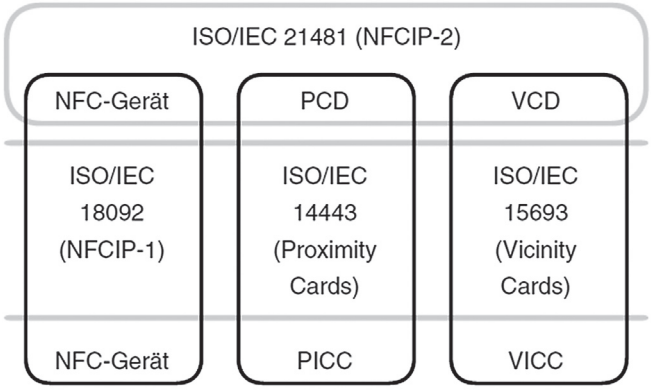


Abb. 1: RFID- und NFC- Normen im Zusammenhang [1]

Komponenten

An einem Angriff sind in der Regel verschiedene Komponenten beteiligt. Bei einem Angriff durch NFC ist zunächst das entsprechende Smartphone zu nennen. Über ein solches Gerät wird mittels einer speziellen Anwendung der Angriff durchgeführt. Hierfür kann jedoch nicht jedes NFC-fähige Smartphone verwendet werden. Viele der heute am Markt verfügbaren Geräte unterstützen nur die Standards im Proximitybereich. Bibliotheken verwenden jedoch Transponder nach Standard ISO 15693, also Vicinity Systeme. Es wird also ein Gerät benötigt, welches es erlaubt auch mit diesem Standard zu kommunizieren. Bisher leisten dies nur wenige Mobiltelefone.

Ein Beispiel dafür ist das Google Nexus S, welches auch für das Testen der Angriffe verwendet wurde. Die bereits erwähnten Transponder sind die direkt angegriffene Komponente. Da der ISO Standard 15693 keine extra Sicherheitsmechanismen bietet, lassen sich Speicherinhalte der Transponder von jedem, mit den nötigen Geräten, verändern. Durch die veränderten Transponderwerte können dann auch weitere Teile des Bibliothekssystems »angegriffen« werden. Das Sicherungsgate kann beispielsweise ein unrechtmäßig verändertes AFI-Byte nicht von einem ordnungsgemäß verändertem unterscheiden. Auch der Selbstverbucher und das LMS können nicht erkennen, ob die Werte im Transponderspeicher verfälscht wurden oder nicht. Das heißt über die direkt angegriffenen Transponder können die weiteren Komponenten des RFID-Bibliothekssystems ebenfalls attackiert werden. Welche Möglichkeiten genau bestehen und wie sich diese auswirken wird in den nächsten Abschnitten noch genauer beschrieben werden.

Angriffsszenarien

Dieser Abschnitt beleuchtet nun zwei der Hauptangriffsvarianten genauer. Dabei wird zunächst beschrieben, wie die entsprechenden Angriffe durchgeführt werden können. Zur Vorgangsbeschreibung gibt es zu jeder Variante noch eine Einschätzung hinsichtlich des Bedrohungspotentials und des Schadens, der durch die jeweilige Attacke entstehen kann, gegeben.

AFI-Change

Dieser Vorgang zielt darauf ab den Diebstahlschutz für Medien außer Kraft zu setzen. Wie bereits beschrieben, ist der ISO 15693 Standard ein offener. Das bedeutet die Transponder sind nicht durch kryptographische Methoden gesichert. Daher kann ein Angreifer ohne weiteres den Transponderinhalt und damit auch das AFI-Byte umschreiben. Für diesen Vorgang kann ein NFC-Smartphone mit entsprechender Applikation genutzt werden. Um dem AFI-Byte einen anderen Wert zu geben muss lediglich die Anwendung gestartet werden und das Smartphone kurz an das Buch gehalten werden. Das Gerät handelt dabei dann als ein RFID-Reader. Ein solcher Angriff dauert in der Regel nur einen sehr kurzen Moment und ist damit auch sehr unauffällig durchführbar.

Mediennummernlotterie

Diese Variante zielt auf das System an sich. Da das Bibliothekssystem mit den sogenannten Mediennummern arbeitet, sind hier auch Angriffspunkte zu finden. Über die Mediennummer aus dem Transponder wird der Bezug zum eigentlich Medium hergestellt.

Ein Angreifer kann nun ebenfalls mit Hilfe eines NFC-Smartphones und einer Anwendung die Mediennummer im Transponder verändern. Auch hier übernimmt das NFC-Smartphone die Rolle des RFID-Readers und ändert die Werte im Transponderspeicher. Je nach Applikation können hier zufällige Nummernkombinationen, manuelle Eingaben oder auch stets die gleiche Nummer verwendet werden.

Bedrohungspotential

Das Bedrohungspotential dieser Angriffe ist unterschiedlich zu bewerten. Der AFI-Change stellt objektiv gesehen zunächst die größere Bedrohung dar. Das hat mehrere Gründe. Eine für diesen Angriff benötigte Anwendung gibt es zwar noch nicht im Internet, kann aber mit wenigen Mitteln selbst erstellt werden. Die Durchführung eines solchen Angriffs erfolgt zudem sehr schnell, da das Umschreiben insgesamt nur wenige Sekunden benötigt. Ein weiterer Punkt ist die Unauffälligkeit des Vorgangs. Ein solcher Angriff könnte rein theoretisch auch mit einem standardmäßigen RFID-Reader durchgeführt werden. Ein solcher ist jedoch relativ groß im Vergleich zu einem Smartphone und muss durch einen Computer gesteuert werden. Damit würde man doch sehr schnell auffallen, was abschreckend wirkt. Mit einem Mobiltelefon tritt dieser Fall nicht ein. Ein Mobiltelefon hat heute fast jeder ständig dabei. Deshalb ist es nicht ungewöhnlich, wenn ein Besucher der Bibliothek mit einem Smartphone in der Hand an den Regalen steht.

Ein weiterer Grund, neben der Einfachheit und Unauffälligkeit dieses Angriffes, für das hohe Bedrohungspotential ist der Schaden, der dabei angerichtet werden kann. Durch das Außerkraftsetzen des Diebstahlschutzes können die Medien ohne Alarm durch die Sicherungstore bewegt und damit aus der Bibliothek entwendet werden. Gerade bei sehr hochwertigen Medien können dabei schnell hohe Schadenssummen entstehen.

Durch den fehlenden Alarm am Gate hat die Bibliothek zudem keine Übersicht über die entwendeten Exemplare, weshalb diese als noch in der Bibliothek vorhanden geführt werden, jedoch nicht zur Verfügung stehen. Man könnte nun dagegen argumentieren, dass für einen solchen Angriff entsprechendes Hintergrundwissen nötig ist. Das ist natürlich in gewissem Maße richtig. Um das System auszuhebeln muss der Angreifer zunächst davon Kenntnis haben, dass ein solcher Angriff überhaupt möglich ist. Und er muss um das Prinzip des AFI-Bytes als Diebstahlschutz wissen. Das sind jedoch nur kleinere Hürden. Begründet ist dies dadurch, dass es bereits eine kommerzielle Applikation für die Ausleihe über ein NFC-Smartphone getestet wird. Das heißt, es ist damit gezeigt, dass es möglich ist. Das »Wie« kann dann sehr schnell über das Internet recherchiert werden. Es bleibt deshalb bei der Gefahreneinschätzung hoch.

Das Bedrohungspotential der Mediennummernlotterie ist geringer einzustufen, als der AFI-Change. Das hat mehrere Gründe. Einer der Gründe ist der Anreiz, der von diesem Angriff ausgeübt wird. Da dieser Angriff nicht darauf abzielt Medien zu entsichern und aus der Bibliothek zu entwenden, ist dieser Angriff wohl eher für eine kleinere Gruppe interessant. Die Erfahrung zeigt, dass zu dieser Gruppe die Personen gehören, die Angriffe auf Systeme durchführen, nur um ihre Fähigkeiten zu testen oder zu testen, was sich mit einem solchen Angriff anrichten lässt. Was einen solchen Angriff ebenfalls weniger interessant werden lässt, ist das zusätzliche Wissen, was dafür benötigt wird. Als erstes muss ein Angreifer das Prinzip der Mediennummern kennen. Das allein reicht jedoch nicht aus. Er benötigt ebenfalls die Stelle im Speicherbereich, in dem die Mediennummer hinterlegt ist. Diese beiden Informationen sind notwendig aber nicht geheim. Wenn ein Angreifer sich mit der Materie intensiv beschäftigt, kann er sich das Wissen selbst aneignen. Dann müsste für das ändern der Mediennummer eine entsprechende Anwendung programmiert werden. Aber auch hier entstehen einige Hürden mehr. Es müssen hier mehrere Werte verarbeitet werden. Für diesen Angriff müssen zuerst Werte gelesen werden und anschließend die Transponder in den ausgewählten Medien umgeschrieben werden. Die Anwendung gestaltet sich damit komplexer. Das wirkt sich natürlich auf die nötige Zeit für die Erstellung aus, welche damit länger wird. Dennoch steigt sie nicht übermäßig an. Die Auswirkung dieses Angriffes ist kein Diebstahl wie beim AFI-Change. Dieser Angriff zielt darauf ab das Bibliothekssystem an sich durch die gefälschten Mediennummern zu stören, sobald ein angegriffenes Medium automatisch ausgeliehen werden soll. Ist die Mediennummer eines Mediums verändert, kann das Bibliothekssystem das reale Exemplar nicht mehr mit dem richtigen Eintrag in der Datenbank in Verbindung bringen.

Das heißt, es wäre zwar noch möglich ein Buch auszuleihen aber in der Datenbank würde ein anderes vermerkt werden. Bei nur wenigen Exemplaren fällt dies eventuell nicht sofort auf. So könnten die falschen Einträge dazu führen, dass Bücher die noch in der Bibliothek stehen, nicht mehr über Suchfunktionen gefunden werden können, weil sie als ausgeliehen gelten.

Ist ein großer Teil der verfügbaren Medien von diesem Angriff betroffen, könnte eine automatische Ausleihe über RFID vermutlich zum erliegen gebracht werden, da die Datenbank die Änderungen nicht kompensieren kann. Für das Bedrohungspotential bedeutet

das, dass es nicht als gering eingeschätzt werden kann. Die Voraussetzungen für diesen Angriff sind zwar höher als beispielsweise beim AFI-Change aber die Auswirkungen sind dennoch verheerend, wenn man den Ausfall des Systems in Betracht zieht. Das Bedrohungspotential wird deshalb mit mittel bis hoch bewertet.

Als Gegenargument könnte man anführen, dass Bibliotheken häufig mehrere Tausend oder sogar mehrere Hundertausend Medien besitzen und diese nicht ohne weiteres alle umgeändert werden können. Dies ist wohl richtig, wenn man von einem einzelnen Angreifer ausgeht. Es würde sich bei einer Zeit von etwa zwei Sekunden, für den reinen Umschreibevorgang, eine Zeit von über 55 Stunden bei 100.000 Medien ergeben. Für einen Einzelnen ein sehr hoher Aufwand. Geht man aber davon aus, dass solch ein Angriff von einer Gruppe durchgeführt wird, wird der Aufwand für jeden Einzelnen wieder schnell kleiner. Deshalb führt der zeitliche Aufwand der Durchführung hier nicht zu einer Herabstufung des Gefährdungspotentials. Ein weiterer Aspekt dieses Angriffes ist die Behebung. Ausgangspunkt für die Betrachtung ist eine Verfälschung der Mediennummern, eines großen Teils des Bestandes. Wenn nun auffällt, dass eine Veränderung an den Nummern vorliegt, muss diese auch wieder behoben werden. Das kann einen enormen Aufwand für die Mitarbeiter der Bibliothek bedeuten. Als erstes müssen nun die betroffenen Medien identifiziert werden. Um zu gewährleisten, dass keine Falschausleihen mehr durchgeführt werden, müsste dazu der gesamte Bestand untersucht werden. Das ist deshalb nötig, da nicht zu erkennen ist welche Bücher genau betroffen sind. Anschließend müssten die korrekten Mediennummern gesucht und wieder in den Transponder geschrieben werden. Dies allein bedeutet einen Zeitaufwand über mehrere Manntage, wenn man wieder von 100.000 Exemplaren ausgeht. Hinzu kommt, dass Mitarbeiter in dieser Zeit nicht ihren normalen Tätigkeiten nachkommen können.

Gegenmaßnahmen

In diesem Abschnitt werden nun einige Möglichkeiten aufgezeigt, wie sich solche Angriffe verhindern lassen könnten. Es handelt sich dabei um Ansätze, die jeweils für eine Bibliothek bewertet werden müssen. Das ergibt sich daraus, dass bestimmte Szenarien nur für gewisse Typen von Bibliotheken geeignet sind.

Verbot von Smartphones

Die erste vorgestellte Variante ist das Verbot von Mobiltelefonen. Diese Option sieht vor, den Benutzern das Mitnehmen von Smartphones in den Bibliotheksbereich zu verbieten. In den meisten Bibliotheken gibt es bereits ein Verbot für Taschen. Diese müssen vor dem Betreten abgelegt werden. Dafür gibt es häufig gesonderte Bereiche mit abschließbaren Fächern, in denen die Rucksäcke und Taschen verstaut werden können. Ein solches Verbot würde Angriffe auf das Bibliothekssystem verhindern, da die Geräte zur Durchführung fehlen würden. In dieser Hinsicht wäre der Effekt natürlich optimal. Es ergeben sich aber hier durchaus auch negative Aspekte, beziehungsweise Schwierigkeiten, die bei einem Verbot bedacht werden müssen.

Zu bedenken ist, dass ein solches Verbot einen deutlichen Einschnitt in die Freiheiten des Bibliotheksbenutzers darstellt. Eine Tasche oder einen Rucksack abzugeben, ist für viele wohl eher ein kleines Übel. Ein Smartphone zu verbieten, könnte jedoch auf wesentlich weniger Verständnis stoßen. Das liegt zum einen an der vielseitigen Nutzung der neuen Telefone. Für viele ist es heute weit mehr als nur ein Telefon, was durch die Bezeichnung Smartphone klar wird. So wird mit solchen Geräten heute häufig das Internet genutzt, gechattet, Musik gehört oder auch navigiert. Da viele heute die eben beschriebenen Möglichkeiten nutzen, dürfte es schwierig werden, die Benutzer dahingehend zu sensibilisieren, auf ihr Smartphone für die Dauer des Bibliotheksaufenthaltes zu verzichten. Solch ein Verbot könnte sich also eher negativ auf die Benutzerzufriedenheit auswirken.

Ein anderer Gesichtspunkt sind die positiven Nutzungsmöglichkeiten von NFC innerhalb der Bibliothek. Wie bereits erwähnt, wurde bereits eine Applikation getestet, die es Nutzern ermöglicht, ein Buch ganz offiziell über ihr Smartphone auszuleihen. Diese Option wäre durch ein Verbot natürlich ebenfalls nicht möglich. Aber auch weitere Dienste wären ohne ein geeignetes Gerät nicht möglich. So könnten beispielsweise Tags mit Standortinformationen an den Regalen angebracht werden.

Diese könnten nicht nur helfen den Benutzer durch die Bibliothek zu navigieren, sondern auch Informationen zur im Regal enthaltenen Literatur zur Verfügung zu stellen.

Eine Navigation würde nicht nur in großen Bibliotheken einen Vorteil bringen. Auch in kleineren Bibliotheken könnten neue Benutzer so besser zu einem gesuchten Medium geleitet werden. Ebenso wäre eine Applikation denkbar, die beim Lesen eines Buchtransponders Verweise auf ähnliche Literatur oder Benutzerbewertungen gibt. Ein Verbot von Smartphones würde also alle eventuellen zusätzlichen NFC-Dienste ebenfalls unmöglich machen. Aber nicht nur die Behinderung von Zusatzdiensten und die Benutzerzufriedenheit stellen dabei negative Aspekte dar. Auch die logistischen Rahmenbedingungen sind nicht zu vernachlässigen. So müssten, um eine solche Maßnahme durchzusetzen, Mitarbeiter abgestellt werden, die dafür verantwortlich sind. Diese müssten die Besucher auffordern bei ihnen ihre Mobiltelefone abzugeben. Es wäre dabei dann nötig, die Telefone dem Besucher zuzuordnen und entsprechend gesichert zu verwahren. Dieser Umstand ist nicht zu unterschätzen, da dafür permanent Mitarbeiter eingesetzt werden müssen. Und nicht nur die Mitarbeiter sondern auch Lagerplatz für die Telefone ist einzurichten. Dieses System hat auch noch andere Schwachstellen. Für eine hundertprozentige Umsetzung müssten Besucher kontrolliert werden, ob sie ihr Gerät auch wirklich abgegeben haben. Aber eine Personenkontrolle durchzuführen ist rechtlich nicht einfach umzusetzen. Dieser Aufwand würde für eine einfache Bibliothek wohl nicht gerechtfertigt sein. Außerdem würde man damit die Zufriedenheit der Besucher wohl deutlich senken.

Einschätzung der Variante Verbot

Wie gesehen, erzeugt ein Verbot einige Schwierigkeiten. Für eine einfache öffentliche Bibliothek oder auch Hochschulbibliothek, wird diese Maßnahme als nicht geeignet

angesehen. Der Zusatzaufwand, der sich durch die Anforderungen an Mitarbeiter und Lagerraum stellt sowie die Einschränkung der Benutzer und Zusatzmöglichkeiten, steht wohl nicht im Gegensatz zu den eventuellen Schäden. Anders könnte sich dies für eine Bibliothek mit hochwertigen Medien darstellen. Bei Sicherung von wertvollen Medien könnte ein Verbot von Mobiltelefonen eher einsetzbar sein. Das begründet sich zum einen schon durch den höheren Wert der Medien, zum anderen sind die Besucherzahlen dort häufig nicht so hoch wie in anderen Bibliotheksformen. Dadurch ließe sich eine Abgabe von Geräten leichter realisieren als in Bibliotheken mit hohen Benutzerzahlen.

Es ist deshalb abzuwiegen, ob der Aufwand für die Durchsetzung eines Verbotes, vor allem dem wirtschaftlichen Nutzen angemessen gegenüber steht.

Verschlüsselung

Eine weitere Möglichkeit den AFI-Change und die Mediennummernlotterie deutlich zu erschweren, ist der Einsatz von Transpondern, die die Möglichkeit der Verschlüsselung bieten. Zunächst ist zu sagen, dass diese Variante nicht in bestehende Transponder nachgerüstet werden kann. Es ist nur möglich neue Transponder in die Medien einzubringen. Durch diese Transponder kann dann jeder Zugriff auf Daten des Chips unterbunden werden, sofern nicht der entsprechende Schlüssel im anfragenden Gerät vorliegt. Ein Umschreiben des AFI-Bytes oder auch das Ändern von Mediennummern wäre so nicht ohne weiteres möglich. Es gilt auch hier, dass eine Verschlüsselung wie jedes andere System keine hundertprozentige Sicherheit bietet. Die verwendeten Verschlüsselungsverfahren, wie beispielsweise Triple Data Encryption Standard (3DES), erfordern einen Aufwand zum Aufbrechen, der einen extremen Zeitaufwand und außerordentliche Rechenleistung benötigen würde.

Als einsetzbare Transponder kommen mehrere Varianten in Frage. Transponder mit Verschlüsselung gibt es heute größtenteils im Bereich von ISO 14443. Das sind solche Transponder, wie sie auch bei Benutzerausweisen oder ähnlichen datenschutzkritischen Karten verwendet werden. Der Einsatz dieser Transponder bringt zu den Vorteilen auch einige Nachteile mit sich. Um mit diesen Tags zu arbeiten, müsste ebenfalls die verwendete Hardware umgerüstet werden. Da ein Bibliothekssystem mit ISO 15693 Transpondern arbeitet, sind natürlich auch die entsprechend passenden RFID-Reader für diesen Standard in Selbstverbucher und Gate integriert. Für die Kommunikation müssen also ebenfalls neue Reader eingebaut werden. Für ein Gate ergibt sich eine zusätzliche Schwierigkeit. Da die ISO 14443 Transponder nur für sehr kurze Distanzen ausgelegt sind, ist es nicht möglich ein Gate zur Sicherung zu verwenden. Durch diesen Umstand sind solche Transponder nicht zum herkömmlichen Diebstahlschutz geeignet. Sie könnten dennoch für die Ausleihe verwendet werden.

Durch den offenen Standard im Bereich ISO 15693 waren die ISO 14443 Transponder im HF-Bereich lange Zeit die einzigen, die eine Verschlüsselung ermöglichten. Seit neuestem gibt es aber auch im Bereich ISO 15693 Möglichkeiten eine Verschlüsselung durchzuführen.

Dabei werden proprietäre Verfahren genutzt, um die Transponder zu verschlüsseln, da solche Verfahren nicht im ISO Standard vorgesehen sind.

Eingesetzt werden solche Chips momentan eher im Bereich von Kartentranspondern. Es wäre aber auch möglich diese Chips in einfache Papierlabel zu integrieren. Obwohl diese Label sich am ISO 15693 Standard orientieren, ist es nötig Anpassungen an der bestehenden RFID-Hardware vorzunehmen. Die Reader können die Transponder zwar erkennen aber durch die Verschlüsselung nicht auf diese zugreifen. Daher muss, wenn möglich, der Algorithmus mit zugehörigem Schlüssel im Reader des Selbstverbuchers nachgerüstet werden. Ist eine Nachrüstung nicht möglich, müssen zu den Transpondern auch die entsprechenden Reader angeschafft und implementiert werden.

Den Vorteil den diese Transponder zu denen im Bereich von ISO 14443 besitzen, ist die Tatsache, dass die Reichweite hier größer ist. Diese wird auch nicht durch die Verschlüsselung eingeschränkt. Daher kann ein solcher Transponder ganz normal auch für den Diebstahlschutz eingesetzt werden, da auch die Funktionalität des AFI implementiert ist. Für die reine Diebstahlsicherung würden dabei am Gate keine Änderungen vorgenommen werden müssen. Sollen aber auch zusätzliche Informationen, wie die Mediennummer, bei gesicherten Transpondern ausgelesen werden, müsste auch hier nachgebessert werden. Es müssten dann die gleichen Veränderungen durchgeführt werden, wie bei den Selbstverbuchern.

Sonst könnten die Reader in den Sicherungsgates nicht auf die Daten der verschlüsselten Transponder zugreifen.

Einschätzung der Variante Verschlüsselung

Eine Verschlüsselung zu benutzen, ist zunächst als sehr positiv zu bewerten. Das Schutzniveau, welches dadurch erreicht wird, ist deutlich höher als eines bei unverschlüsselten Transpondern. Dadurch könnten also für einen längerfristigen Zeitraum Angriffe über NFC vermieden werden.

Zu beachten ist jedoch bei der Variante mit den ISO 14443 Transpondern die eingeschränkte Nutzungsmöglichkeit. Durch die Tatsache, dass die Transponder nicht wie gewohnt über ein Gate zur Sicherung eingesetzt werden können, würde ein erheblicher Einschnitt entstehen. Der Einsatz dieser Transponder ist also, wenn überhaupt, nur in speziellen Fällen empfehlenswert. Vom Funktionsumfang und damit der Einsatzfähigkeit her betrachtet stellen die neuen ISO 15693 Transponder, mit proprietärer Verschlüsselung eine wesentlich bessere Alternative dar. Diese Transponder wären, durch die Konformität zum ISO Standard, gut für den Einsatz in allen Arten von Bibliotheken geeignet. Der Schutz der dadurch erzielt werden könnte, würde Angriffe wie AFI-Change und die Mediennummernlotterie wirksam verhindern können. Damit ist der Einsatz von verschlüsselten Transpondern dieser Art zunächst durchaus positiv zu bewerten.

Diese Variante hat jedoch auch negative Aspekte, die ebenfalls betrachtet werden müssen. Solche Transponder sind durch die Komplexität entsprechend teurer, als

herkömmliche Transponder. Teilweise sind die Preise für solche Transponder um das Drei- oder Vierfache höher. In Bibliotheken, in denen ein RFID-System eingesetzt werden soll, muss also zunächst analysiert werden, ob der höhere Anschaffungswert überhaupt aufzubringen ist und dem Nutzen angemessen gegenüber steht. Ein weiterer Punkt der nicht unerheblich ist, ist die Tatsache, dass sich die Verschlüsselung nicht nachträglich in die Transponder integrieren lässt. Dieser Umstand bringt für Bibliotheken, die bereits RFID eingeführt haben einen großen Nachteil mit sich. Würde man die neuen Transponder einsetzen wollen, müsste man zunächst noch einmal Investieren um die Tags zu beschaffen. Dabei können, wie eben gesehen, schnell sehr hohe Summen anfallen. Das zweite Problem ist, dass diese Transponder in die Medien eingebracht werden müssen. Für die Bibliotheksmitarbeiter bedeutet dieser Umstand, dass der gesamte Bestand wieder die Konvertierung durchlaufen muss.

Hier entsteht ein nicht zu unterschätzender Personalaufwand. Durch die Bindung der Mitarbeiter in der Konvertierung entstehen natürlich auch zusätzliche Personalkosten. Ein Beispiel hierfür bildet die folgende Rechnung. Ausgegangen wird dabei von einer Bibliothek mit einem Bestand von 200.000 einfachen Printmedien. Ein Team aus zwei Mitarbeitern benötigt die für die Konvertierung die folgenden Arbeitskraftstunden (AKh):

200.000 / 3.500 Bücher pro Tag, zwei Personen und 8AKh 912AKh

Für weitere Einflussgrößen wie Fehlen, Rüstzeiten oder Marge des Anbieters muss ein zusätzlicher Faktor eingerechnet werden. Dieser wird mit 1,3 angesetzt.

Daraus ergibt sich: 912AKh * 1,3 = 1.185AKh

Die Arbeitszeit allein, die für eine Konvertierung aufgewendet werden muss, ist bereits beträchtlich. Nimmt man nun einen Satz von 24€/h Vollkosten an, bedeutet dass, eine Summe 28.440€ für die berechneten AKhs. [vgl. 2] Auch hier entstehen also deutliche Kosten. Diese bereits einmal durch die Einführung von RFID in den Bibliotheken entstanden. Sollte nun das System auf verschlüsselte Transponder umgerüstet werden, würden diese Zeiten und Kosten abermals anfallen.

Was ebenfalls noch negativ ins Gewicht fallen kann, ist die Tatsache, dass es bisher nur wenige Anbieter solcher Transponder gibt und sich eine Bibliothek unter Umständen in Sachen Transponder von einem Hersteller abhängig machen könnte.

Zusatzdatenbank

Dieser letzte Lösungsansatz arbeitet nicht wie die vorher gezeigten Varianten mit der Sicherung von Transpondern. Es wird hier eine zusätzliche Datenbank genutzt, die auf einer Änderung der Arbeitsweise des Bibliothekssystems basiert. Bisher arbeitet der Großteil der Bibliothekssysteme mit den Mediennummern, die im Transponder hinterlegt sind. Diese werden zur Zuordnung der Transponder zu den Einträgen im LMS genutzt. Weiterhin wird das AFI-Byte verwendet um Medien mit Hilfe eines Gates vor Diebstählen zu sichern. Durch diese Arbeitsweise werden jedoch auch die vorgestellten Angriffe erst ermöglicht. Um nun einen solchen Angriff zu verhindern, ist es, wie gezeigt, möglich die

Transponder selbst zu sichern. Es gibt jedoch auch die Möglichkeit das System an sich anzupassen. Der erste Schritt dabei ist, von den Daten des Transponders nur die UID zu verwenden. Dadurch lassen sich die oben gezeigten Angriffe, die auf das AFI-Byte oder auch die Mediennummer abzielen, wirksam verhindern. Da die UID nicht veränderbar ist, kann diese auch nicht über ein NFC-fähiges Smartphone angegriffen werden.

Damit ist ein zunächst sehr einfacher Mechanismus zur Sicherung gefunden. Um diese Art des Schutzes nutzen zu können, müssen jedoch noch weitere Umstellungen vorgenommen werden. Auch das LMS muss an die neue Situation angepasst werden. Dazu muss sofern dies möglich ist, anstatt einer Mediennummer die UID des Transponders in der Datenbank gespeichert werden. Beziehungsweise ist es auch möglich, weiterhin eine Mediennummer zu benutzen. Diese wird dann nur innerhalb des LMS verwendet und mit der zughörigen Seriennummer des Tags abgeglichen. So können an einem Selbstverbucher die UIDs der Medientransponder ausgelesen und an das LMS gesendet werden. Im LMS werden, wie sonst auch, die Daten abgeglichen und die Informationen zu den Medien zurück an den Selbstverbucher gesendet. Damit ist die Funktion der Selbstausleihe gewährleistet. Um die Sicherung der Medien zu gewährleisten wird eine entsprechende Datenbank verwendet. Für eine solche Datenbank gibt es unterschiedliche Möglichkeiten.

Als eine Variante könnte die Datenbank sämtliche UIDs der Medien der Bibliothek enthalten. Zu diesen wird dann der entsprechende Status gespeichert, also ob ein Medium gesichert oder entliehen ist. Wird nun am Selbstverbucher eine Ausleihe getätigt, wird nicht nur das LMS angesprochen, sondern auch die Datenbank, die nur den Status enthält. Dieser wird entsprechend gesetzt. Wird nun das Medium durch ein Sicherungsgate getragen, wird vom Transponder nicht das AFI-Byte, sondern die Seriennummer gelesen. Diese wird dann an die Datenbank gesendet und verglichen.

Ist das Medium nicht ordnungsgemäß entliehen, wird ein Alarm aktiviert. Da Transponder die zu anderen Anwendungen gehören nicht in der Datenbank sind, wird bei diesen auch kein Fehlalarm ausgelöst. Für die Umsetzung dieser Funktionalität müssen selbstverständlich Änderungen an den Komponenten vorgenommen werden.

Die Datenbank muss zunächst erstellt und eingerichtet werden. Da eine solche Datenbank relativ wenige Daten verarbeiten muss, sind auch die Anforderungen an die benötigte Hardware nicht außerordentlich. Für die Sicherung über ein Gate muss eine Verbindung zwischen der neuen Datenbank und dem Gate selbst bestehen. Wichtig ist, dass die Verbindung zwischen Gate und Datenbank sehr schnelle Antwortzeiten ermöglicht. Das ist notwendig, um auch zum richtigen Zeitpunkt einen Alarm auszulösen und diesen nicht verzögert anzuregen, zum Beispiel wenn sich das betreffende Medium bereits nicht mehr im Gate befindet.

Es muss zusätzlich eine weitere Verbindung vom Selbstverbucher zur Datenbank eingerichtet werden, um den Status für ein entliehenes Medium oder ein zurückgebuchtes Medium zu aktualisieren. Dadurch, dass das Gate nun nicht mehr allein für die Sicherung zuständig ist, sind auch hier die neuen Abläufe zu implementieren. Im günstigsten

Fall lassen sich diese ohne Probleme mit der bestehenden Firmware umsetzen. Ist dies nicht möglich, ist es nötig eine für diesen Anwendungsfall passende Firmware zu entwickeln.

Eine zweite Variante für eine Speicherung des Status von Medien wäre die Vorhaltung der Informationen direkt im Reader des Sicherungsgates. Dabei wird, im Gegensatz zum vorhergehenden Fall, keine zusätzliche Hardware benötigt. In der Regel besitzen RFID-Reader in Sicherungsgates einen sogenannten Pufferspeicher. In diesem können Transpondernummern abgespeichert werden. Diese Möglichkeit erlaubt es nun die Diebstahlsicherung zu gewährleisten. Dazu wird eine zusätzliche Verbindung vom Selbstverbucher zum Gate eingerichtet. Diese dient dazu die UIDs von ausgeliehen Medien in den Pufferspeicher des Reader zu sichern und umgedreht, bei Rückbuchungen, diese zu entfernen. Wird nun ein Medientag im Gate erkannt, welcher nicht im Pufferspeicher hinterlegt ist, gibt das Gate einen Alarm. Es kann dafür nötig sein, einen größeren Speicher nachzurüsten oder Reader mit größeren Speichern anzuschaffen. Da der Speicher jedoch im Reader integriert ist sollten an dieser Stelle keine Zeitprobleme beim Überprüfen des Status auftreten.

Die Umstellung der Arbeitsweise ist hier etwas schwieriger. Die Transponder können zwar bei einer Ausleihe oder Rückbuchung entsprechend ausgelesen und dann einen Eintrag in der Datenbank erhalten, dies setzt aber voraus, dass die Daten noch nicht verfälscht wurden.

Das Gate müsste für die Zeit der Umstellung dann entweder zusätzlich noch über AFI sichern oder bei jedem Transponder der nicht in der Datenbank ist einen Alarm geben. Dadurch würde gewährleistet, dass bisher noch nicht erfasste Transponder gesichert sind. Andernfalls wäre es nötig, den gesamten Bestand zu erfassen. Liegen die Zuordnungen zwischen Medium und UID bereits in irgendeiner Weise vor, kann dies jedoch auch schnell und einfach implementiert werden.

Einschätzung der Variante Zusatzdatenbank

Zunächst ist zu sagen, dass der Schutz, der durch die Änderung der Arbeitsweise erreicht werden kann, sehr hoch ist. Für Angreifer ist es nicht möglich, mittels NFC die UID von Transpondern zu verändern. Und da weder AFI-Byte noch Medienummer auf dem Tag verwendet werden, lassen sich auch darüber keine Angriffe mehr durchführen. Damit liegt der Schutz noch höher als bei den Varianten, die mit Verschlüsselung, Passwort oder anderen Sicherheitsmerkmalen arbeiten. Ein weiterer Vorteil ist, dass keine neuen Transponder angeschafft werden müssen. Somit müssen für diese keine Mittel für Beschaffung und Nachlabeln aufgewendet werden, was gegenüber Verschlüsselung eine erhebliche Einsparung darstellt. Die zusätzlich benötigte Hardware für Datenbank und Verbindungen ist in diesem Fall unwesentlich klein. Wie angesprochen, müssen hier auch Änderungen am LMS vorgenommen werden. Da aber wie bisher die Datensätze weiter verwendet werden können, muss nur eine zusätzliche Verknüpfung zwischen Mediennummer und UID eingeführt werden.

Die beiden genannten Varianten besitzen beide Vor- und Nachteile. Bei der ersten Option können keine fremden Transponder Fehlalarme auslösen, da alle UIDs in der Datenbank hinterlegt sind. Allerdings können hier bei langsamer Verbindung oder Verarbeitung ungewollte Verzögerungen entstehen. Die zweite Option bietet schnellen Zugriff auf die gespeicherten Transponder. Da sich hier jedoch nur die ausgeliehenen Transponder im Speicher befinden, werden auch Alarme ausgelöst, wenn anwendungsfremde Tags durch das Gate gebracht werden. Nach heutiger Technik sollte die Verbindung zwischen Gate und Datenbank jedoch so aufzubauen sein, dass die benötigten Vorgaben erfüllt werden, weshalb diese Variante zu empfehlen ist. Auch wenn die Implementierung einige Risiken bergen kann, ist der erreichte Schutz ausgezeichnet. Bei Bibliotheken die ein System neu einführen, würde dieser Schritt bei der Konvertierung der Medien, mit angepasster Konvertierungssoftware, mit durchgeführt werden können.

Fazit

NFC findet mittlerweile immer stärkere Verbreitung in verschiedenen Anwendungsgebieten. Durch die Integration in neue Generationen von Smartphones gibt es nun quasi den RFID-Reader für jedermann. Auch wenn bisher noch andere Probleme in Bibliotheken überwiegen, wird es in Zukunft wichtig sein sich auch mit diesem Thema auseinander zu setzen. Die hier beschriebenen Angriffe zeigen welche Folgen NFC für eine Bibliothek mit RFID-System haben kann. Es ist deshalb wichtig sich schon frühzeitig um eine ausreichende Sicherung zu bemühen. Die hier gezeigten Maßnahmen stellen nur die ersten Ansätze dar und müssen von Bibliothek zu Bibliothek nach den entsprechenden Vorgaben auf Umsetzbarkeit untersucht werden.

Literatur und Internetquellen

[1] Roland, Michael/Langer, Joseph (2010). Anwendungen und Technik von Near Field Communication (NFC), Springer-Verlag Berlin, Heidelberg

[2] Kern, Christian (2011). RFID für Bibliotheken, Springer-Verlag, Berlin, Heidelberg

Der elektronische Identitätsnachweis
Einsatzmöglichkeiten des neuen Personalausweises im privat-wirtschaftlichen Umfeld

Marian Margraf

Personalausweise werden heute nicht nur zur Feststellung z. B. der Identität bei der Grenz- oder Personenkontrolle durch Polizei oder Zoll eingesetzt, sondern finden auch häufig im privatwirtschaftlichen Umfeld Anwendung. Die im Chip des zukünftigen elektronischen Personalausweises enthaltenen Funktionen a) elektronischer Identitätsnachweis und b) qualifizierte elektronische Signatur, werden dafür sorgen, dass die herkömmliche Nutzung von Personalausweisen in der »Papierwelt« auf die elektronische Welt übertragen wird. Der Artikel geht auf die Hauptideen des elektronischen Identitätsnachweises ein, erläutert insbesondere die Unterschiede zur qualifizierten elektronischen Signatur und zeigt konkrete Einsatzszenarien.

1. Einleitung

Ab 01.11.2010 wird der neue Personalausweis in Deutschland ausgegeben. Wesentliche Neuerungen dieses Dokumentes sind, neben der zukünftigen Form im Scheckkartenformat, die Integration eines kontaktlosen Chips mit ISO 14443-Schnittstelle, der sowohl eine Anwendung für den hoheitlichen Bereich enthält, z. B. im Rahmen einer Grenzkontrolle, als auch zwei Anwendungen für die Nutzung im privatwirtschaftlichen Umfeld. Einen Überblick über die elektronischen Funktionen gibt Abb. 1.

Bei der Gestaltung der elektronischen Funktionen wurden in besonderer Weise die Anforderungen an Datenschutz und Datensicherheit beachtet und umgesetzt. Ein zuverlässiger Schutz personenbezogener Daten kann nur durch ein Zusammenspiel rechtlicher Bestimmungen, organisatorischer Maßnahmen und technischer Umsetzungen gewährleistet werden. Auch für die bisherige Nutzung des Ausweises in der Papierwelt hat das bis heute gültige Personalausweisgesetz verschiedene Bestimmungen zum Umgang mit dem Dokument vorgesehen. So ist z. B. eine Kopie des Ausweises nur in Ausnahmefällen gestattet. Die Seriennummer eines Ausweises darf nicht für einen automatisierten Abgleich in Datenbanken genutzt werden und der maschinenlesbare Bereich steht außerhalb hoheitlicher Anwendungen nicht zur Verfügung.

Identifizierung für hoheitl. Anwendungen	**Authentisierung** für E-Business/E-Govern.	**Signatur** für E-Business/E-Govern.
Gesichtsbild Fingerabdruck Name, Vorname Geburtsdatum usw.	Name, Vorname Adresse Alter/Altersverifikation Pseudonym usw.	qualifizierte elektronische Signatur nach deutschem Signaturgesetz

Abb. 1: Überblick über die elektronischen Funktionen des neuen Personalausweises.

Diese Regelungen wurden in dem neuen Personalausweisgesetz übernommen. Darüber hinaus müssen aber, gerade für die Absicherungen der neuen elektronischen Funktionen, zusätzliche Sicherheitsmechanismen realisiert werden. Daher wurden bei dem Design der Funktionen des Chips insbesondere die folgenden Anforderungen umgesetzt:

- Eine Datenübermittlung erfolgt stets verschlüsselt.
- Datenübermittlungen erfolgen nur im Einvernehmen mit dem Inhaber.
- Eine Nutzung des Personalausweises durch Dritte ist nicht möglich.
- Der Inhaber weiß, wem gegenüber er seine Daten übermittelt.
- Es werden nur die Daten übermittelt, die auch benötigt werden.
- Die Nutzung kann weder von einer staatlichen noch von anderen Stellen überwacht werden.
- Mit dem Personalausweis ist auch eine pseudonyme Anmeldung möglich.
- Ein globales eindeutiges, den Personalausweis oder den Inhaber zuordenbares Merkmal, existiert nicht.

Gerade der letzte Punkt erfordert eine besondere Umsetzung zur Sperrung abhanden gekommener Ausweise, siehe Abschnitt 3.3.

In den folgenden Kapiteln werden die elektronischen Funktionen des neuen Personalausweises im Einzelnen beschrieben, wobei hauptsächlich auf den elektronischen Identitätsnachweis und dessen Unterschiede zur qualifizierten elektronischen Signatur eingegangen wird. Zum Abschluss werden dann mögliche Einsatzszenarien erläutert.

2. Anwendungen des Personalausweises im privatwirtschaftlichen Umfeld

Neben der Feststellung der Identität bei der Grenz- oder Personenkontrolle, z. B durch Polizei oder Zoll, werden Personalausweise auch regelmäßig im privatrechtlichen Umfeld genutzt. Der Grundgedanke ist dabei immer derselbe. Der Ausweisinhaber weist sich gegenüber einer anderen Person, hier z. B. gegenüber einem Geschäftspartner oder einem Behördenvertreter, mit dem für seine Person ausgestellten Dokument aus und zeigt damit, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Üblicherweise ist Ausweisinhabern bekannt, wem gegenüber sie ihre Identität nachweisen. Im geschäftlichen oder behördlichen Umfeld betritt man die Räumlichkeiten einer Institution oder lässt sich von der Person gegenüber ebenfalls einen Ausweis zeigen. Auf dieser Grundlage nehmen Ausweisinhaber an, dass die Personen gegenüber im Auftrag der so verkörperten Institutionen handeln.

Es findet also eine gegenseitige Authentisierung statt. Bei dieser Art des Identitätsnachweises handelt es sich allerdings lediglich um eine Momentaufnahme, bei der keine der beiden Parteien ohne weiteres im dauerhaften Besitz eines von Dritten anerkannten Beweises über die Identität und den Willen des anderen bleibt. Ein solcher Beweis wird durch eine eigenhändige Unterschrift geschaffen, welche bei Bedarf in Verwaltungs- oder Gerichtsverfahren herangezogen werden kann.

Ziel des neuen Personalausweises, der seit 01.11.2010 in Deutschland ausgegeben wird, ist es, diese herkömmliche Nutzung von Ausweisen in der »Papierwelt« auf die elektronische Welt auszuweiten. Dazu stehen optional zwei Funktionen für Diensteanbieter im E-Government- und E-Businessbereich zur Verfügung:

Der elektronische Identitätsnachweis (kurz eID-Funktion) realisiert eine gegenseitige Authentisierung zweier Kommunikationspartner über das Internet, so dass jede Partei weiß, mit wem sie kommuniziert.

Die qualifizierte elektronische Signatur (kurz QES) nach deutschem Signaturgesetz stellt das Äquivalent zur eigenhändigen Unterschrift im elektronischen Rechts- und Geschäftsprozess dar.

2.1. Der elektronische Identitätsnachweis

Nach der Definition aus dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist Authentisierung ein Vorgang oder Verfahren zur Überprüfung und Bestätigung einer Identität.

Geschieht dies auf Seiten des Dienstanbieters beim bisherigen Personalausweis durch Sichtprüfung der Sicherheitsmerkmale und Abgleich des Gesichtsbildes, müssen in der elektronischen Welt andere Mechanismen gefunden werden. Die Prüfung von Sicherheitsmerkmalen, d. h. das Überprüfen, ob ein echter Personalausweis vorliegt, kann durch geeignete kryptographische Echtheitsnachweise geschehen.

An Stelle der Überprüfung der Übereinstimmung körperlicher Merkmale (Abgleich des Gesichtsbildes) tritt in der elektronischen Welt die Eingabe einer geheimen PIN. Durch diesen Prozess beweist der Besitzer des Personalausweises auch Inhaber, d. h. rechtmäßiger Besitzer des Personalausweises zu sein.

Ein weiteres Ziel ist, dass sich nicht nur der Personalausweisinhaber gegenüber einem Dienstanbieter authentisiert, sondern auch der Dienstanbieter gegenüber dem Personalausweisinhaber; die Authentisierung soll also gegenseitig sein. Dies geschieht über so genannte Berechtigungszertifikate, die Dienstanbieter erhalten. In diesem ist neben Angaben zur Gültigkeit des Zertifikates, zum Inhaber des Zertifikates auch ein öffentlicher Schlüssel und die Kategorien der Daten, die der Dienstanbieter vom Chip des Personalausweises lesen darf, enthalten.

Diese Zertifikate erhalten Dienstanbieter von einer staatlichen Stelle, der Vergabestelle für Berechtigungszertifikate (VfB), die beim Bundesverwaltungsamt (BVA) betrieben wird. Dabei muss der Dienstanbieter ein berechtigtes Interesse nachweisen, personenbezogene Daten aus dem elektronischen Personalausweis auszulesen. Das berechtigte Interesse wird innerhalb einer Erforderlichkeitsprüfung festgestellt und stellt die Voraussetzung für die Vergabe von Berechtigungszertifikaten dar. Wesentliches Ziel dieses Verwaltungsaktes durch die VfB ist auch zu prüfen, welche der auf dem Chip des Ausweises gespeicherten Daten der Diensteanbieter auslesen darf. Beispielsweise erhalten Dienste, die eine Altersverifikation durchführen müssen, lediglich Zugriff auf das Datum, das beschreibt, ob der Inhaber ein gewisses Alter über- oder unterschritten hat. Andere Dienste, wie zum Beispiel Online-Versandhäuser, können darüber hinaus auch Zugriff auf Daten wie Name, Vorname und Wohnadresse erhalten.

2.2. Qualifizierte elektronische Signatur

Die elektronische Authentisierung mit der eID-Funktion des elektronischen Personalausweises soll die erforderliche Sicherheit und das Vertrauensverhältnis zwischen Anbietern und Nutzern elektronischer Dienste im Internet herstellen. Im Unterschied zum elektronischen Identitätsnachweis wird mit der eigenhändigen Unterschrift eine dauerhafte Zurechenbarkeit zu den unterzeichnenden Personen erreicht. Wird durch ein gesetzliches Schriftformerfordernis im Geschäftsverkehr bzw. Verwaltungsverfahren gemäß § 126 a Absatz 1 BGB bzw. einschlägiger Vorschriften des Verwaltungsverfahrensgesetzes ein dauerhaft zurechenbarer Beweis über die Abgabe einer Willenserklärung oder einer Handlung in der elektronischen Welt gefordert, bedarf es der qualifizierten elektronischen Signatur.

Eine wesentliche Rolle spielen dabei die Abschluss- und Warnfunktion der eigenhändigen Unterschrift als Bestätigung von übereinstimmenden Willenserklärungen. Diese dient insbesondere der Klarheit darüber, den Inhalt eines Rechtsgeschäfts verstanden und akzeptiert zu haben sowie im Streitfalle einen hinreichenden Beweis führen zu können. Dabei sollen die Vertragsparteien mit dem Akt der Unterzeichnung zugleich gewarnt werden, voreilig Verträge abzuschließen.

Der neue Personalausweis ist als sichere Signaturerstellungseinheit nach dem deutschen Signaturgesetz ausgestaltet, so dass Personalausweisinhaber jederzeit bei Bedarf ein qualifiziertes elektronisches Zertifikat auf den Chip des Personalausweises von einem Trust-Center laden lassen können.

2.3. Beispiel für die Anwendung von eID-Funktion und QES

Das nachfolgende, vereinfacht dargestellte Beispiel, soll die Übertragung der heutigen Funktionen des Personalausweises in die elektronische Welt darstellen.

Möchte ein Bankkunde ein Konto eröffnen, muss dieser heute in der Regel unter Vorlage eines gültigen Ausweisdokuments zum Identitätsnachweis persönlich erscheinen. Gemäß § 4 Abs. 4 GWG kann die Identität bei natürlichen Personen »... anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird...« geprüft werden. Mit dem Betreten der Bank vertraut der Bankkunde auf die Handlungsvollmacht der Bankmitarbeiter. Damit findet eine gegenseitige Authentisierung zwischen Kunde und Bank statt. Die Authentisierung ist dabei lediglich eine Momentaufnahme. Erst mit dem anschließenden Vertragsschluss zwischen Bank und Kunde erhält die Willenserklärung Beweiskraft. Mit Verabschiedung des PAuswG wird § 6 Abs. 2 Nr. 2 Satz 1 des GWG in der Weise ergänzt, dass die persönliche Vorlage eines Personalausweises durch die Nutzung des elektronischen Identitätsnachweises ersetzt werden kann.

Dank dieser Gesetzesänderung könnte der Prozess künftig online wie folgt abgebildet werden:

Schritte	Kontoeröffnung klassisch	Kontoeröffnung online
1. Schritt = Identitätsnachweis (eID-Funktion)		
Bank weist ihre Identität nach	Der Kunde betritt die Geschäftsräume einer Bank	Personalausweis prüft Berechtigungszertifikat der Bank
Kunde weist seine Identität nach	Personalausweis wird vom Bankangestellten geprüft.	Bank prüft elektronisch Sicherheitsmerkmale, Chip übersendet (verschlüsselt) die benötigten Daten
2. Schritt = Unterschrift (QES-Funktion)		
Abschluss des Vertrages zur Kontoführung	Der Kunde und der Bankangestellte unterschreiben den Kontoführungsvertrag.	Mit der QES-Funktion des Personalausweises und der QES eines Angestellten der Bank wird ein Vertrag über die Kontoführung signiert.

Tab.1: Vergleich klassischer und elektronischer Kontoeröffnung mit dem Personalausweis.

3. Technische Umsetzung des elektronischen Identitätsnachweises

Grundidee der eID-Funktion ist, zwischen Chip des neuen Personalausweises und Dienstanbieter einen authentisierten Diffie-Hellman-Schlüsselaustausch ablaufen zu lassen. Damit werden zwei Ziele erreicht:

- Beide Kommunikationspartner wissen, mit wem sie kommunizieren (Authentizität).
- Zwischen den Kommunikationspartnern wird ein gemeinsames Geheimnis ausgetauscht, so dass ein verschlüsselter und authentischer Kanal aufgebaut werden kann (Schlüsselaustausch).

Um zu erreichen, dass das Diffie-Hellman-Verfahren auch authentisiert ist, müssen die öffentlichen Schlüssel dem jeweiligen Kommunikationspartner zugeordnet werden können. Dies geschieht, wie im Folgenden beschrieben, über elektronische Signaturen und, um eine Bindung zwischen Inhaber und Ausweis zu garantieren, der Nutzung der nur dem Inhaber des Ausweises bekannten geheimen PIN.

Genaue Beschreibungen der kryptographischen Protokolle finden sich in der Technischen Richtlinie TR 03110, siehe [5], Anforderungen an die Mindestschlüssellänge der jeweiligen Verfahren in der Technischen Richtlinie TR 02102, siehe [6].

3.1. PACE (PIN-Eingabe)

Eine Kommunikation mit dem Chip des neuen Personalausweises kann nur dann stattfinden, wenn der Ausweisinhaber vorab seine geheime, nur ihm bekannte PIN eingegeben hat und damit einwilligt, seine Identität nachzuweisen. Dadurch wird eine sogenannte Zwei-Faktor-Authentisierung umgesetzt, die auf Besitz (Personalausweis) und Wissen (PIN) basiert.

Das zur Eingabe der PIN verwendete Protokoll PACE (Password Authenticated Connection Establishment) sorgt gleichzeitig für eine verschlüsselte Verbindung zwischen kontaktlosem Chip des Ausweises und lokalem Lesegerät, so dass weder personenbezogene Daten noch die PIN von Dritten mitgelesen werden können. Ein Sicherheitsbeweis dieses Protokolls findet sich in [1].

3.2. EAC (Terminal- und Chip-Authentisierung)

3.2.1. Terminal Authentisierung (Authentisierung des Diensteanbieters)

Zunächst ist der Dienstanbieter, wie bereits beschrieben, im Besitz eines Berechtigungszertifikats, das u. a. Name des Dienstanbieters und einen öffentlichen Schlüssel beinhaltet. Der zu diesem öffentlichen Schlüssel zugehörige geheime Schlüssel muss in einem sicheren Speicherbereich der Systemumgebung beim Dienstanbieter abgelegt werden. Weiter ist auf den Chips der neuen Personalausweise ein Rootzertifikat des BSI gespeichert, mit dem die Gültigkeit der Berechtigungszertifikate (über eine Zertifikatskette) überprüft werden kann.

Für den Verbindungsaufbau mit einem Ausweis erzeugt der Dienstanbieter ein variables Diffie-Hellman-Schlüsselpaar. Der öffentliche (Diffie-Hellman)-Schlüssel wird vom Dienstanbieter mit dem geheimen Schlüssel signiert, der zum Schlüsselpaar des Berechtigungszertifikats gehört. Diese Daten, d. h. das Berechtigungszertifikat (und die weiteren Zertifikate bis zum Rootzertifikat), der öffentliche Diffie-Hellman-Schlüssel und die zugehörige Signatur, werden zum Chip des Personalausweises gesendet.

Der Chip
- prüft die kryptographische Gültigkeit des Berechtigungszertifikates,
- prüft, ob der Dienstanbieter im Besitz des geheimen Schlüssels ist (durch ein Challenge-Response-Verfahren[1]) und
- prüft die Signatur des o. g. öffentlichen (Diffie-Hellman)-Schlüssels.

Danach weiß der Personalausweisinhaber, mit welchem Dienstanbieter er kommuniziert und dass dieser die Berechtigung erhalten hat, Daten aus dem Personalausweis anzufragen.

3.2.2. Chip-Authentisierung (Nachweis der Echtheit des Ausweises)

Der Chip des Personalausweises besitzt ein statisches Diffie-Hellman-Schlüsselpaar. Der geheime (Diffie-Hellman-)Schlüssel befindet sich in einem sicheren Speicherbereich im Chip des elektronischen Personalausweises, so dass er weder ausgelesen noch kopiert werden kann.

Der zugehörige öffentliche (Diffie-Hellman-)Schlüssel wird mit dem geheimen Schlüssel des Ausweisherstellers im Zuge der Personalisierung des Ausweises signiert. Für diesen Zweck erhält der Ausweishersteller vom BSI ein Zertifikat mit den entsprechenden Schlüsseln, d. h. auch für diese Zertifikate bildet das BSI die Root und autorisiert den Ausweishersteller zur Erstellung hoheitlicher Dokumente.

Diese Signatur wird vom Dienstanbieter durch Prüfung der Zertifikatskette bis zum Rootzertifikat verifiziert, so dass der Dienstanbieter nach erfolgreicher Prüfung weiß, dass er mit einem echten Personalausweis kommuniziert.

Um das Tracking eines elektronischen Personalausweises zu verhindern, werden Personalausweise, die während eines bestimmten Zeitraumes ausgestellt werden (z. B. im Zeitraum von drei Monaten) mit dem selben Diffie-Hellman-Schlüsselpaar ausgestattet. Ein chipkartenindividuelles Schlüsselpaar würde Dienstanbieter in die Lage versetzen, Personalausweise zu erkennen, ohne dass personenbezogene Daten überhaupt übermittelt werden. Die Sicherheit ist von dieser Lösung nicht betroffen. Im Gegensatz zu vielen anderen Lösungen authentisiert sich der Ausweisinhaber nicht über ein eindeutiges Schlüsselpaar, wie zum Beispiel in einem Challenge-Response-Protokoll, sondern, wie im folgenden Abschnitt beschrieben, über Teile der im Chip gespeicherten Daten. Das Diffie-Hellman-Schlüsselpaar dient den Dienstanbietern lediglich dazu, festzustellen, dass ein echter Personalausweis vorliegt.

3.2.3 Authentisierung des Inhabers

Nach beiderseits erfolgreichem Austausch der signierten, öffentlichen Diffie-Hellman-Schlüssel (Diffie-Hellman-Schlüsselaustausch) kann jede Seite mit dem eigenen geheimen Diffie-Hellman-Schlüssel und dem öffentlichen Diffie-Hellman-Schlüssel der

1 Dieses Verfahren dient der Authentisierung und dem Nachweis, dass der Diensteanbieter im Besitz des ihm zugeteilten geheimen Schlüssels ist. Der Ausweischip erzeugt eine Zufallszahl und sendet diese an den Diensteanbieter. Dieser signiert diese Zufallszahl mit dem geheimen Schlüssel, der zum Schlüsselpaar des Berechtigungszertifikats gehört. Der Ausweischip prüft entsprechend die Signatur mit dem dazugehörigen öffentlichen Schlüssel.

Gegenseite das gleiche kryptographische Geheimnis erzeugen. Aus diesem Geheimnis werden kryptographische Schlüssel zur Authentisierung und Verschlüsselung der zu übertragenden personenbezogenen Daten abgeleitet (Secure Messaging).

Die verschlüsselte Datenübertragung erfolgt mit dem symmetrischen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard) im CBC-Mode. Authentisiert wird die Datenübertragung durch die Verwendung von AES-CMAC (Cipher Message Authentication Code), womit die Vertraulichkeit und Authentizität der zu übertragenden elektronischen Daten gewährleistet wird.

Der Dienstanbieter kann im Ergebnis der Übermittlung sicher sein, dass die an ihn übermittelten Daten aus einem echten Personalausweis stammen. Aufgrund der Trennung Besitz (Personalausweis) und Wissen (PIN) kann der Dienstanbieter davon ausgehen, dass der Personalausweisinhaber diesen willentlich selbst verwendet. Damit hat sich schließlich auch der Personalausweisinhaber gegenüber dem Dienstanbieter authentisiert.

Umgekehrt hatte sich der Dienstanbieter bereits zuvor über sein Berechtigungszertifikat gegenüber dem Personalausweisinhaber authentisiert. Zusätzlich weiß der Personalausweisinhaber dank der verschlüsselten Kommunikation, dass nur der berechtigte Dienstanbieter seine ausgewählten personenbezogenen Daten erhält.

3.3. Sperrmanagement

3.3.1. Sperrung von Personalausweisen

Um die missbräuchliche Nutzung gestohlener oder verloren gegangener Personalausweise zu verhindern, können diese gesperrt werden. Dazu muss ein eindeutiges, ausweisindividuelles Merkmal während des elektronischen Identitätsnachweises zum Diensteanbieter gesendet werden, damit Personalausweise, die sich in einer Sperrliste befinden, vom Dienstanbieter als gesperrte Ausweise erkannt werden können.

Auf der anderen Seite soll ein Tracking des Ausweises verhindert werden. Ein eindeutiges Sperrmerkmal unterläuft diese Anforderung allerdings (aus dem selben Grund werden, wie Abschnitt 3.2.3 beschrieben, die Ausweischips auch nicht mit einem eindeutigen Schlüsselpaar ausgestattet). Eine Lösung dieses »Widerspruchs« ist die Verwendung von diensteanbieterspezifischen Sperrlisten, d. h. jeder Ausweis übersendet während des elektronischen Identitätsnachweises ein dienste- und kartenspezifisches Sperrmerkmal an den Dienstanbieter, den dieser gegen seine diensteanbieterspezifische Sperrliste abgleicht. Die zentrale Sperrliste, aus der diensteanbieterspezifische Listen berechnet werden, wird beim Bundesverwaltungsamt betrieben. Der genaue Prozess ist wieder in [5] beschrieben.

Ein Tracking von Ausweisen über ein globales Personalausweismerkmal ist somit ausgeschlossen.

3.3.2. Sperrung von Berechtigungszertifikaten der Dienstanbieter

Da der Chip des Personalausweises nur über begrenzte Ressourcen verfügt, ist es nicht möglich, Berechtigungszertifikate vom Dienstanbieter, deren Berechtigung zurückgezogen wurde, über eine Rückrufliste zu sperren. Daher ist hierfür ein anderer Mechanismus vorgesehen, der allerdings das gleiche Sicherheitsniveau garantiert.

Berechtigungszertifikate werden für eine sehr kurze Zeit ausgestellt (i. d. R. ein bis zwei Tage). Die Gültigkeit der Schlüssel ist im Berechtigungszertifikat enthalten. Der Chip des Ausweises speichert lediglich den Gültigkeitsbeginn des hoheitlichen Zertifikates, welches als letztes akzeptiert wurde. Wird ein Berechtigungszertifikat vorgelegt, dessen Gültigkeitszeitraum vor diesem gespeicherten Zeitpunkt liegt, wird dieses zurückgewiesen. Ein Entzug der Berechtigung für einen Dienstanbieter kann damit durch das Nicht-Ausstellen weiterer Berechtigungszertifikate geschehen.

4. Infrastruktur

Die Nutzung der eID-Funktion im E-Government und E-Business setzt eine reibungslos funktionierende Infrastruktur voraus, wie z. B. die für Zertifikate und deren Sperrung benötigte Public Key Infrastruktur, an der eine Reihe von Behörden und Institutionen beteiligt sind. Dazu gehört insbesondere das BSI als Betreiber der Root-CAs, das BVA mit der VfB und dem Sperrdienst, TrustCenter, die die eigentliche technische Ausstellung der Berechtigungszertifikate übernehmen, die Bundesdruckerei GmbH als Hersteller der neuen Ausweise und die Hotline, die einfache Fragen zu den neuen Funktionen des Ausweises beantwortet und Sperrmeldungen abhanden gekommener Ausweise annimmt.

Wesentliche Komponenten für eine erfolgreiche Etablierung der eID-Funktion im privatwirtschaftlichen Umfeld sind zum einen der sogenannte Bürgerclient, eine Software, mit denen Bürgerinnen und Bürger den Chip des Ausweises erst nutzen können und zum Zweiten der sogenannte eID-Server, der es Diensteanbietern ermöglicht, die Nutzung der eID-Funktion einfach in ihre bereits existierenden IT-Systeme zu integrieren.

4.1. AusweisApp

Mit der AusweisApp stellt die Bundesregierung allen Bürgerinnen und Bürgern eine Softwarekomponente zur Nutzung der elektronischen Funktionen des neuen Personalausweises kostenfrei zur Verfügung. Kern dieser Software ist das eCard-API-Framework, das eine interoperable Nutzung von Signatur-, Authentisierungs- und Verschlüsselungsanwendungen, die auf unterschiedlichen Chipkarten (kontaktbehaftet, kontaktlos) realisiert sein können, garantiert, vergleiche [4]. Damit wird es zukünftig möglich sein, nicht nur den neuen Personalausweis zu nutzen, sondern auch bereits im Feld befindliche Lösungen sowie zukünftige Karten schnell und kostengünstig zu integrieren.

Die AusweisApp wird derzeit für alle gängigen Betriebssysteme, wie z. B. Windows XP, Vista und 7, Mac OS X und einige Linuxversionen (OpenSuse, Ubuntu, Debian) bereit gestellt und unterstützt die am häufigsten auf diesen Systemen genutzten Internetbrowser, sowie, zur Signatur und Verschlüsselung, alle gängigen E-Mail-Programme.

Weitere Informationen zum Bürgerclient finden sich auf den Internetseiten des Kompetenzzentrums »Neuer Personalausweis« unter www.ccepa.de.

4.2. eID-Server

Wie bereits oben beschrieben, soll der eID-Server die Integration der elektronischen Funktionen des neuen Personalausweises und aller weiteren, vom Bürgerclient unterstützten Karten, in die bereits bestehenden IT-Systeme der Diensteanbieter vereinfachen. Der eID-Server übernimmt dabei die gesamte Kommunikation mit der beim Bürger genutzten Karte. Die Kommunikation zur VfB zum Erhalt von Berechtigungszertifikaten und zum Sperrlistenbetreiber (dem BVA) zum Erhalt seiner Sperrlisten wird ebenfalls vom eID-Server übernommen. Ein Diensteanbieter muss somit nur noch eine sichere Verbindung zwischen seinem Web-Server und einem eID-Server etablieren (über ihm bereits bekannte Protokolle wie z. B. SSL oder SAML).

Spezifiziert ist der eID-Server in [9], weitere Informationen finden sich unter www.ccepa.de.

4.3. Wissens- und Kommunikationsplattform

Auf der Wissens- und Kommunikationsplattform sollen sich sowohl Bürgerinnen und Bürger, als auch Diensteanbieter umfassend über alle Themen rund um den neuen Personalausweis informieren. Für Diskussionen, auch zu kritischen Fragen, steht zusätzlich ein moderiertes Internetforum zur Verfügung. Das Internetangebot findet man unter www.personalausweisportal.de.

5. Nutzungsmöglichkeiten in Bibliotheken

Ein wesentlicher Vorteil des elektronischen Identitätsnachweises ist die Nutzung einer sicheren Chipkarte auch ohne vorherige Registrierung für einen bestimmten Dienst. Dies lässt sich am Beispiel einer Online-Bibliothek einfach erläutern: Für einen Zugriff auf ein beschränktes Internetportal, auf dem z. B. elektronische Zeitschriften und Lehrbücher nur für Mitarbeiterinnen, Mitarbeiter und Studierende der jeweiligen Hochschule bereitgestellt werden, müssen sich heute die Nutzer vorab für diesen Dienst anmelden. In der Regel wird dazu ein amtlicher Ausweis bzw. ein Mitarbeiterausweis oder die Studienbescheinigung benötigt. (Dieses Vorgehen ähnelt dem Verfahren zum Erhalt eines herkömmlichen Bibliotheksausweises.) Nach dem erfolgreichen Registrierungsprozess vergibt die Bibliothek dann login und Passwort (in wenigen Bibliotheken auch eine sichere Chipkarte), der Nutzer ist erst danach in der Lage, sich mit diesen Daten an dem Portal anzumelden und den Dienst zu nutzen. Dies lässt sich zukünftig deutlich einfacher und

sicherer mit dem neuen Personalausweis gestalten. Ähnliches gilt für viele Prozesse an Hochschulen, wie z. B. Anmeldungen zu Prüfungen, Einsicht in Prüfungsergebnisse usw.

So wie Nutzer heute mit Hilfe des Personalausweises ihre Identität gegenüber einem Vertreter der Bibliothek nachweisen, können sie dies zukünftig unter Nutzung des elektronischen Identitätsnachweises ohne persönliches Erscheinen in der Bibliothek an ihrem Heim-PC. Mit einem entsprechenden Berechtigungszertifikat können die für die Anwendung notwendigen Daten, wie z. B. Name, Vorname, Adresse, aus dem Chip des Ausweises ausgelesen werden. Diese Daten können dann mit einer hochschulinternen Datenbank abgeglichen werden, um eine Mitgliedschaft der betreffenden Person zu der Hochschule zu verifizieren und gegebenenfalls den Status (d. h. Professor, wissenschaftlicher Mitarbeiter, Studierender) feststellen zu können. Abhängig von dem Ergebnis können dann spezielle Zugriffsrechte innerhalb des Portals freigegeben werden.

Literatur

[1] Jens Bender, Dennis Kügler, Marian Margraf & Ingo Naumann (2008). Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DuD, Datenschutz und Datensicherheit, 32(3): 850–864.

[2] Jens Bender (2009). Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[3] Jens Bender, Marc Fischlin und Dennis Kügler (2009). Security Analysis of the PACE Key-Agreement Protocol. Information Security Conference (ISC) 2009, Lecture Notes in Computer Science, Volume 5735, pp. 33-48, Springer-Verlag.

[4] Detlef Hühnlein & Manuel Bach (2008). Die Standards des eCard-API-Frameworks. DUD, Datenschutz und Datensicherheit, 32(6): 379-382.

[5] Dennis Kügler (2009). Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.02. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[6] Marian Margraf (2008). Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[7] Marian Margraf (2009). Der elektronische Identitätsnachweis des zukünftigen Personalausweises. in: 19. SIT-SmartCard Workshop (Fraunhofer-Institut für Sichere Informationstechnologie), Darmstadt 3./4. Februar 2009, pp. 3-14.

[8] Alexander Roßnagel, Gerrit Hornung & Christoph Schnabel (2008). Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht. DuD, Datenschutz und Datensicherheit, 32(3): 850–864.

[9] BSI (2009). Technische Richtlinie TR-03130, eID-Server, Version 1.0. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

Technische Richtlinien des BSI finden Sie auf www.bsi.bund.de.

Abkürzungsverzeichnis

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AFI	Application Family Identifier
AFL	aktive Fernleihe
ALA	American Library Association
API	Application Programming Interface
ASRS	Automated Storage and Retrieval System
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CCC	Chaos Computer Club
CD	Compact Disc
CIP	Competitiveness and Innovation Framework Programme
CMAC	Cipher Message Authentication Code
CBRS	Centre national de la recherche scientifique (Nationales Zentrum für wissenschaftliche Forschung – Frankreich)
DIHK	Deutscher Industrie- und Handelskammertag e. V.
DIMDI	Deutsches Institut für medizinische Dokumentation und Information
DIN	Deutsches Institut für Normung / Deutsche Industrie Norm
DIS	Draft International Standard
DTD	Document Type Definition
DVD	Digital Versatile Disc
DVD	Deutsche Vereinigung für Datenschfutz e. V.
EAC	Extended Access Control
EAS	Electronic Article Surveillance
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFF	Electronic Frontier Foundation
EFRE	Europäischer Fond für Regionale Entwicklung
eID	elektronische Identitätsnachweis
ENISA	European Network and Information Security Agency
EU	Europäische Union
FDIS	Final Draft International Standard
FIfF	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung
Fitug	Förderverein Informationstechnik und Gesellschaft
FoeBuD	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.
GID	Gesellschaft für Information und Dokumentation
GOLEM	Großrecherorientierte, listenorganisierte Ermittlungsmethode
GRIPS/DIRS	General Relation Based Information Processing System / Document Information Retrieval System
HF	High Frequency
ICNIRP	International Commission on Non-Ionizing Radiation Protection

IF ..... Informationsforum RFID e. V.
ILL ..... Interlibrary Loan
IP ..... Internet Protocol
ISIL ..... International Standard Identifier for Libraries and Related Organizations
ISM ..... Industrial, Scientific and Medical
ISO ..... International Organization for Standardization
LAN ..... Local Area Network
LF ..... Low Frequency
LMS ..... Library Management System
LVO ..... Leihverkehrsordnung
MHz ..... Mega Hertz
NCIP ..... National Information Standards Organization Circulation Interchange Protocol
NFC ..... Near Field Communication
NISO ..... National Information Standards Organization
NSM ..... Neues Steuerungsmodell
OID ..... Object Identifier
OPAC ..... Online Public Access Catalogue
PACE ..... Password Authenticated Connection Establishment
PAuswG ..... Personalausweisgesetz
PDA ..... Personal Digital Assistant
PFL ..... passive Fernleihe
PR ..... Public Relations
QES ..... qualifizierte elektronische Signatur
RFID ..... Radio-Frequency Identification
RTLS ..... Real Time Locating System
SIP2 ..... Standard Interchange Protocol
SLNP ..... Simple Library Network Protocol
STAIRS ..... Storage and Information Retrieval System
TCP/IP ..... Transmission Control Protocol / Internet Protocol
UHF ..... Ultra High Frequency
UID ..... Unique Identification
UMTS ..... Universal Mobile Telecommunications System
USB ..... Universal Serial Bus
VDA ..... Verband der Automobilindustrie
VfB ..... Vergabestelle für Berechtigungszertifikate
VLM ..... Vertical-Lift-Module
VoIP ..... Voice over IP
VÖBB ..... Verbund Öffentlicher Bibliotheken Berlins
VSWR ..... Voltage Standing Wave Ratio
WiBe ..... Wirtschaftlichkeitsbetrachtungen
WLAN ..... Wireless LAN
XML ..... Extensible Markup Language

Autoren

Prof. Dr. Marco Althaus
Technische Hochschule Wildau [FH]
Hochschulring 1, 15745 Wildau
T +49 30 3375 508-341
marco.althaus@th-wildau.de

Anke Berghaus-Sprengel
Leiterin Abteilung Zweigbibliotheken
Universitätsbibliothek der Humboldt-Universität zu Berlin, Jacob-und-Wilhelm-Grimm-Zentrum
Geschwister-Scholl-Str. 1/3, 10117 Berlin
T +49 30 2093-99290
anke.berghaus-sprengel@ub.hu-berlin.de

Josef Bernhard
Fraunhofer Institut für Integrierte Schaltungen
Nordostpark 93, 90411 Nürnberg
T +49 9131 776-0
josef.bernhard@iis.fraunhofer.de

Dipl.-Ing. Daniel Büth
System Application Engineer
FEIG ELECTRONIC GmbH
Lange Str. 4, 35781 Weilburg
T +49 6471 31090
daniel.bueth@feig.de

Catherine Cooke
Senior Business Systems Analyst
Westminster Libraries
Marylebone Library, Marylebone Road,
London NW1 5PT, England
T +44 20 7641-1206
ccooke@westminster.gov.uk

Tobias Dräger
Fraunhofer Institut für Integrierte Schaltungen
Nordostpark 93, 90411 Nürnberg
T +49 9131 776-0
tobias.draeger@iis.fraunhofer.de

Olaf Eigenbrodt
Leiter Hauptabteilung Benutzungsdienste und Baubeauftragter
Staats- und Universitätsbibliothek Hamburg Carl von Ossietzky
Von-Melle-Park 3, 20146 Hamburg
T +49 40 42838-3344
olaf.eigenbrodt@sub.uni-hamburg.de

Prof. Dr. Achim Enders
Technische Universität Braunschweig,
Institut für Elektromagnetische Verträglichkeit
Schleinitzstr. 23, 38106 Braunschweig
T +49 531 391-7722
achim.enders@tu-braunschweig.de

Prof. Dr.-Ing. Frank Gillert
Leiter Forschungsgruppe Sichere Objektidentität
Technische Hochschule Wildau [FH]
Hochschulring 1, 15745 Wildau
T +49 3375 508-240
frank.gillert@th-wildau.de

Dr.-Ing. Michał Grabia
Institute of Logistics and Warehousing (ILiM)
Estkowskiego 6, 61-755 Poznań, Polen
T +48 618504946
michal.grabia@ilim.poznan.pl

Dipl.-Ing. Dieter Horst
Siemens AG, Industry Sector,
Industry Automation Division
Siemensstr. 2-4, 90766 Fürth
T +49 911 978-2780
dieter.horst@siemens.com

Tomasz Janiak, M.A.
Institute of Logistics and Warehousing (ILiM)
Estkowskiego 6, 61-755 Poznań, Polen
T +48 618504922
tomasz.janiak@ilim.poznan.pl

Dr. Christian Kern
Technik/Geschäftsführung
InfoMedis AG
Brünigstrasse 25, 06055 Alpnach, Schweiz
T +41 41 6170777
christian.kern@infomedis.ch

Guido Kippelt
Hochschule Hamm-Lippstadt
Marker Allee 76-78, 59063 Hamm
T +49 2381 8789-181
guido.kippelt@hshl.de

Jan Kissig
Technische Hochschule Wildau [FH]
Hochschulring 1, 15745 Wildau
T +49 3375 508-941
jan.kissig@th-wildau.de

Doris Köhler
Universitätsbibliothek Bielefeld
Universitätsstr. 25, 33615 Bielefeld
T +49 521 106-3417
doris.koehler@uni-bielefeld.de

Sebastian Krautz
Technische Hochschule Wildau [FH]
Hochschulring 1, 15745 Wildau
T +49 3375 508-649
skrautz@th-wildau.de

Dr. Marian Margraf
Bundesministerium des Innern
Alt-Moabit 101D, 10559 Berlin
T +49 3018 681-0
marian.margraf@bmi.bund.de

Dipl.-Ing. Wolfgang Meißner
Senior Development Engineer
FEIG ELECTRONIC GmbH
Lange Str. 4, 35781 Weilburg
T +49 6471 31090
wolfgang.meissner@feig.de

Barbara Michaelis
aStec GmbH
Paul-Lincke-Ufer-7c, 10999 Berlin
T +49 30 617939-0
bm@astecb.astec.de

Prof. Dr. Ulrich Naumann
Leitender Direktor
Universitätsbibliothek
der Freien Universität Berlin
Garystr. 39, 14195 Berlin
T +49 30 838-54093
naumann@ub.fu-berlin.de

Cathrin Neumair
Bayerische Staatsbibliothek
Ludwigstr. 16, 80539 München
T +49 89 28638-2777
cathrin.neumair@bsb-muenchen.de

Dr. Rainer Sprengel
Freiberuflicher Experte für
bürgerschaftliches Engagement,
Information und Wirtschaftlichkeit
Lermooser Weg 40b, 12209 Berlin
T +49 157 82462112
rainersprengel@online.de

Prof. Dr. Ulrike Verch
Hochschule für Angewandte
Wissenschaften Hamburg
Fakultät Design, Medien & Information
Finkenau 35, 22081 Hamburg
T +49 40 42875-3619
ulrike.verch@haw-hamburg.de

Markus Weinländer
Siemens AG, Industry Sector,
Industry Automation Division
Gleiwitzer Str. 555, 90475 Nürnberg
T +49 911 895-4891
markus.weinlaender@siemens.com

Dipl.-Ing. Hardy Zissel
Technische Hochschule Wildau [FH]
Hochschulring 1, 15745 Wildau
T +49 3375 508-453
hardy.zissel@th-wildau.de

Stichwortindex