Fachhochschule Nordwestschweiz
Hochschule für Life Sciences

Fallstudie Mikrosysteme

Implantierte RFID-Chips und Privatsphäre



Abgabetermin: 06. Juni 2011

Autoren: David Bertschin, David Hilber, Michel Heiniger

Modul: Mikrosysteme

Auftraggeber: Marc Dusseiler

Ort, Datum: Muttenz, 06. Juni 2011

LST Vollzeit 2009

Inhaltsverzeichnis

1 Abstract 1

2 Grundlagen der RFID-Technologie 2

2.1 Geschichte 2

2.2 Funktionsweise 2

2.2.1 Grundprinzip 2

2.3 Heutige & künftige Anwendungen 4

2.4 Wieso RFID? (Vor- /Nachteile) 5

2.4.1 Vorteile: 5

2.4.2 Nachteile: 5

2.5 Anforderungen an implantierbare RFID-Systeme 5

3 Implantierbare RFID-Systeme 6

3.1 Heutige Anwendungen 6

3.1.1 Tieridentifikation: 6

3.1.2 VeriChip / VeriMed: 7

3.1.3 NeuralWISP: 8

3.2 Vor- / Nachteile 9

3.2.1 Vorteile: 9

3.2.2 Nachteile: 10

3.3 Zukünftige Entwicklungen 10

3.3.1 Implantierter Glukose-Sensor und Nanoroboter: 10

3.4 Gefahren und Risiken 13

4 Datenschutz und Privatsphäre 15

4.1 Rechtliche Grundlagen Schweiz 15

4.2 Rechtliche Grundlagen EU 16

4.3 Probleme 16

4.4 Massnahmen 17

4.5 Gesellschaftliche Akzeptanz 18

5 Fazit 20

6 Quellen und Abbildungsverzeichnis.....21

6.1 Quellenverzeichnis.....21

6.2 Abbildungsverzeichnis 22

1 Abstract

Die RFID-Technologie dürfte vor allem durch die kontroverse Diskussion über die biometrischen Reisepässe bekannt geworden sein. Nicht weniger umstritten sind implantierte RFID-Chips, welche neben Bedenken des Datenschutzes auch gesundheitliche Schäden anrichten können. Mit dieser Arbeit wird einerseits diese Problematik thematisiert, andererseits werden auch die Grundlagen der RFID-Chips erklärt. Des Weiteren werden zukünftige Entwicklungen und mögliche Einsatzgebiete vorgestellt, denn trotz aller Kritik steckt in dieser Technologie viel Potential. So wird beispielsweise angenommen, dass mit Hilfe von RFID die Diabetes-Therapie revolutioniert werden kann. Auch für die sogenannte in-vivo Diagnostik wird das Know-How von RFID unumgänglich sein. Diesen interessanten Entwicklungen ist ein Teil gewidmet, doch auch über Datenschutz und Privatsphäre sind spannende Fakten nachzulesen. Zuerst müssen aber die Grundlagen der RFID-Technologie bekannt sein, welche im folgenden Kapitel behandelt werden.

2 Grundlagen der RFID-Technologie

2.1 Geschichte

Die RFID-Technologie wurde erstmals während dem zweiten Weltkrieg von den Briten verwendet um eigene von feindlichen Flugzeugen zu unterscheiden. Dabei sendete man ein Radarsignal aus, dass den Transponder in den Flugzeugen aktivierte und dieser dann ein Signal an das Radar zurücksendete und so die Identifizierung des Flugzeugs ermöglichte.

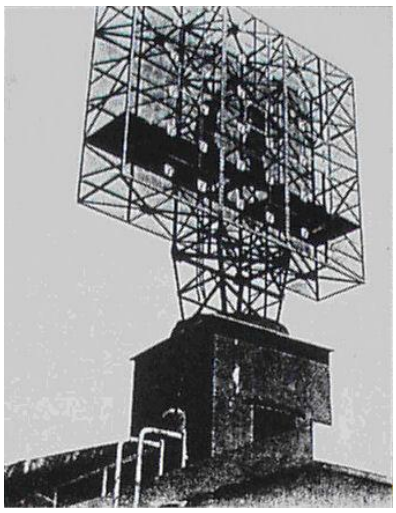


Abbildung 1: Britisches Radar im 2. Weltkrieg

In den siebziger Jahren wurde der erste Vorläufer des heute verwendeten RFIDs entwickelt. Dabei handelte es sich um ein Warensicherungssystem das ein Bit speichern konnte, das für nicht bezahlt oder bezahlt stand. Diese Systeme sind noch heute in den Warenhäusern anzutreffen.

Durch Weiterentwicklung dieser Technologie wurde sie Ende der siebziger in der Landwirtschaft für die Erkennung der der Nutztiere verwendet.

Danach hat man immer weitere Verwendungszwecke für RFID gefunden die im späteren Kapitel näher beschrieben werden. [1]

2.2 Funktionsweise

2.2.1 Grundprinzip

Mit dem RFID Lesegerät kann man entweder lesen oder schreiben. Dabei wird ein hochfrequentes elektromagnetisches Wechselfeld erzeugt, dass sobald ein RFID-Transponder oder Tag genannt in dieses Feld kommt wird dieser aktiviert. Die Energieversorgung erfolgt unterschiedlich. Bei aktiven Tags wird die ganze Energieversorgung durch eine Batterie gewährleistet, bei halbaktiven wird nur der Chip mit von einer Batterie versorgt. Die implantierten RFID-Tags haben meistens keine eigene Energieversorgung. Die Energieversorgung wird über die Antenne die in dem Hochfrequenz Feld des Readers ist, während der Kommunikation gewährleistet. Sobald der Tag und der Reader im gleichen Feld sind werden zuerst die Befehle vom Reader decodiert. Bei der Antwort baut der Tag keine eigens

Wechselfeld auf sondern benutzt das Feld vom Reader in dem es eine Feldschwächung im kontaktfreien Kurzschluss erzeugt. So wird dann z.B. die Identifikation vom Tag übermittelt. Für das RFID stehen insgesamt vier Frequenzen bereit.

- Langwelle: 125-135MHz
- Kurzwelle: 13.56MHz
- UHF(ultra high frequencies): 865-869MHz in Europa
- 950MHz in Asien und den USA
- SHF: 2.45GHz und 5.8GHz

Frequency Ranges	LF 125 KHz	HF 13.56 MHz	UHF 868 - 915 MHz	Microwave 2.45 GHz & 5.8 GHz
Typical Max Read Range (Passive Tags)	Shortest 1"-12"	Short 2"-24"	Medium 1'-10'	Longest 1'-15'
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive storage, E-field coupling	Active tags with integral battery or passive tags using capacitive storage, E-field coupling
Data Rate	Slower	Moderate	Fast	Faster
Ability to read near metal or wet surfaces	Better	Moderate	Poor	Worse
Applications	Access Control & Security Identifying widgets through manufacturing processes or in harsh environments Ranch animal identification Employee IDs	Library books Laundry identification Access Control Employee IDs	supply chain tracking Highway toll Tags	Highway toll Tags Identification of private vehicle fleets in/out of a yard or facility Asset tracking

Abbildung 2: RFID-Frequenzen

Die Hoch Frequenz RFID-Tags benutzen dabei eine Lastmodulation und die UHF-Tags eine Modulierte Rücksteuerung.

Ein Problem bleibt jedoch, dass RFID Tags nicht in jeder Lage gelesen werden können, was bei Verpackungen sehr wichtig wäre denn sonst würde wichtige Zeit verloren gehen um jedes Mal die Verpackung in die richtige Position zu drehen. Dieses Problem hat man damit gelöst, das man den Tag mit einer zirkulierenden Polarisation anspricht und er so ho-

rizontal sowie auch vertikal gelesen werden kann. Jedoch wird bei dieser Technik das Signal-Rausch-Verhalten reduziert.

Die RFID-Tags können auch mit einem GPS Modul gekoppelt werden um genaue Ortsbestimmungen durchführen zu können. [1][2][5]

2.3 Heutige & künftige Anwendungen

- Der wohl bekannteste und sowohl umstrittenste Einsatz von RFID ist in den neuen Schweizer und europäischen biometrischen Pässen, mit auf den Chip gespeicherten Fingerabdrücken und Gesichtsmerkmalen.

Abbildung 3: RFID-Tag

- In Singapur werden sogenannte ePlates benutzt. Das sind Nummernschilder mit eingebautem RFID-Tag. Diese werden benutzt um die Mautgebühren für die Innenstadt zu kontrollieren.

- Zudem werden RFIDs zu Identifizierung und Kennzeichnung von Nutz- und Haustieren benutzt um z.B. entflohene oder streunende Hunde ihrem Besitzer zuordnen zu können. Diese werden den Tieren unter die Haut implantiert.

- Immer häufiger werden RFIDs in kontaktlosen Chipkarten verwendet um zum Beispiel die Eingangskontrolle eines Gebäudes zu regeln.

- Seit einigen Jahren kann man sich einen RFID-Tag implantieren lassen um in einer Disco in Rotterdam in den VIP Bereich zu kommen. Damit kann der Gast dann Bargeldlos bezahlen und kann ohne sich anzustellen in die Disko hinein. [1][2]

2.4 Wieso RFID? (Vor- /Nachteile)

2.4.1 Vorteile:

- Das Auslesen des RFID-Tags erfolgt kontaktlos und es wird keine Sichtverbindung benötigt. Somit gibt es auch keinen Verschleiss und das auslesen wird auch nicht durch Verschmutzung verhindert. Somit ist das ganze System auch Wartungsfrei, bis auf den Reader.
- Es können mehr Informationen gespeichert werden als auf einem simplen Barcode.
- Bei aktiven RFID-Tags mit einem Mikroprozessor können auch Daten verarbeitet werden.
- Die Kommunikation von Tag und Reader kann verschlüsselt werden, somit wird es erschwert von Fremden Tags auszulesen.[4]

2.4.2 Nachteile:

- Gefahr einer persönlichen Vollüberwachung.
- Die Tags können auch von Dritten ausgelesen werden.[4]

2.5 Anforderungen an implantierbare RFID-Systeme

Die RFID-Tags werden subkutan in die Haut eingesetzt. Aus diesem Grund haben die Tags auch andere Anforderungen, als wenn man sie zum Beispiel für Verpackungen verwendet werden. Deshalb werden heutige Chips, die implantiert werden, von einem Glaskörper verhüllt, da Glas hautverträglich ist und vom Körper nicht abgestossen wird.

Jedoch können nach dem implantieren auch Probleme entstehen. Bei Versuchen mit Mäusen denen man einen RFID-Tag implantiert hat, hat sich nach einiger Zeit Krebs an der implantierten Stelle entwickelt.

Ein weiteres Problem ist, wenn man sich mit einem implantierten Chip eine MRI-Untersuchung durchführen lässt. Dabei kann sich der Tag aufheizen, und es kann dadurch zu Verbrennungen kommen. [3]

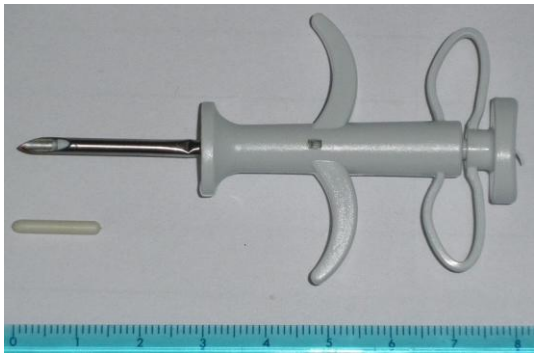
3 Implantierbare RFID-Systeme

Implantierte RFID-Systeme kennt man vor allem von der Tieridentifikation. Dabei werden sie nicht nur bei der Identifizierung von entlaufenen Tieren eingesetzt, sondern auch am Zoll. Auf diese Anwendung wird im folgenden Kapitel nochmals eingegangen, doch das Hauptaugenmerk gilt den RFID-Chips die beim Menschen eingesetzt werden oder zukünftig möglicherweise zum Einsatz kommen. Zudem sollen die Vor- und Nachteile aufzeigt und mögliche Gefahren und Risiken von implantierten Systemen erläutert werden.

3.1 Heutige Anwendungen

3.1.1 Tieridentifikation:

Den meisten Hundebesitzer/innen der Schweiz und in der EU dürfte das System der Tieridentifikation bekannt sein, doch dass dabei RFID-Technik genutzt wird, wahrscheinlich weniger. Jeder Hundehalter/in ist nämlich per Gesetz verpflichtet, seinem Welpen spätestens 3 Monate nach dessen Geburt einen Chip implantieren zu lassen. Er wird dem Tier auf der linken Halsseite unter die Haut implantiert. Injiziert wird der Chip von einem Tierarzt, der dazu eine Spezialspritze verwendet.



Der reiskorngrosse Mikrochip ist in ein Glasgehäuse eingeschlossen um das Gewebe des Tieres zu schützen und eine Immunreaktion zu verhindern. Das Einsetzen des Chips soll nahezu schmerzfrei und vergleichbar mit einer Impfung sein.

Abbildung 4: Spezialspritze

Auf dem Chip werden eine spezifische Nummer und ein Code für die Schweiz gespeichert. Über diese Nummer erhält man Angaben über den Hund sowie dessen Besitzer. Diese Daten werden in einer zentralen Datenbank, dem Animal Identity Service (ANIS) gespeichert.

Der RFID-Chip ist laut ANIS völlig ungefährlich und soll sich weder unter der Haut verschieben, noch zerbrechen. Studien haben jedoch gezeigt, dass diese Mikrochips ein Krebsrisiko für die Tiere sind. Mehr dazu finden sie unter dem Kapitel Gefahren und Risiken. [6]

3.1.2 VeriChip / VeriMed:

Der erste und bislang einzige kommerziell erhältliche RFID-Chip der dem Menschen implantiert werden darf, namens VeriChip, wurde 2004 von der US-amerikanischen Gesundheitsbehörde FDA zugelassen. Er wird von der VeriChip Corporation hergestellt und soll bislang schätzungsweise 2000 Personen implantiert worden sein. Der RFID-Chip trägt die Produktbezeichnung VeriMed, bekannt wurde er aber unter dem Namen VeriChip. Diese Bezeichnung wird auch in dieser Arbeit verwendet.

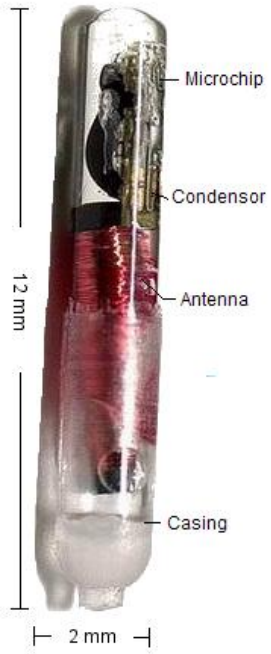


Abbildung 5: VeriChip

Der Aufbau ist identisch zu den Chips die bei Tieren verwendetet werden und lässt sich grob in zwei Teile aufteilen. Einerseits benötigt der Mikrochip eine Antenne die Strom durch Induktion liefert. Dies geschieht über ein Magnetfeld das vom Lesegerät ausgeht und von der Antenne genutzt wird. Über das Magnetfeld wird auch ein Signal an den RFID-Chip gesendet. Dieses Signal wird durch das zweite Bauteil des Systems, dem eigentlichen Mikrochip, moduliert und danach zurückgesendet.

Die genaue Funktionsweise wurde im ersten Kapitel “Grundlagen der RFID-Technologie” erklärt.

Das ganze System wird in eine dicht verschlossene Glaskapsel gepackt und mit einem Kunststoff ummantelt. Die Kunststoffbeschichtung besitzt eine raue Oberfläche, dadurch soll das Implantat mit dem menschlichen Gewebe verwachsen. Durch das Verwachsen versucht man allfällige Verschiebungen des Chips zu verhindern. Üblicherweise wird der VeriChip in die Rückseite des rechten Oberarms oder in die Hautfalte zwischen Daumen und Zeigefinger eingesetzt. Der Chip ist rund 12 Millimeter lang und hat etwa einen Durchmesser von 2 mm. Dies entspricht wahrscheinlich auch den Dimensionen des Hunde-Chips.

Wie bei der Tieridentifikation sind auch auf dem VeriChip keine persönlichen Daten gespeichert. Auf dem Lesegerät wird lediglich eine einzigartige 16-digit Identifikationsnummer abgelesen, welche zu einem Eintrag in einer Datenbank passt. Dieser Eintrag umfasst mehre-

re Angaben über den Implantat Träger, dessen Ansprechpartner und Arzt sowie Informationen über Allergien, Medikation, Implantate und frühere chirurgische Eingriffe.

Der Hersteller nennt folgende Leute als besonders geeignet für den VeriChip:

Personen mit chronischen Krankheiten wie:

- Koronare Herzkrankheit
- Chronisch obstruktive Lungenerkrankung
- Diabetes
- und weitere

Ebenfalls geeignet sind nach Ansicht des Herstellers Personen mit Alzheimer, Implantaten wie Herzschrittmacher etc.

Auf mehreren Internetseiten werden neben gesundheitlichen auch religiöse Bedenken geäussert. Die gesundheitlichen Schäden die ein solches Implantat ausrichten kann, werden unter *Gefahren und Risiken* aufgeführt. Fragen bezüglich *Datenschutz und Privatsphäre* werden im letzten Kapitel beantwortet. [7][8][9][10][11]

3.1.3 NeuralWISP:

Die RFID-Technologie wird nicht nur kommerziell genutzt, sie wird auch in der Forschung eingesetzt. Ein Beispiel dafür ist das NeuralWISP. WISP ist die Abkürzung von Wireless Identification and Sensing Platform. Es handelt sich dabei um ein universelles Sensor-System welches RFID nutzt um die Messresultate zu übertragen.

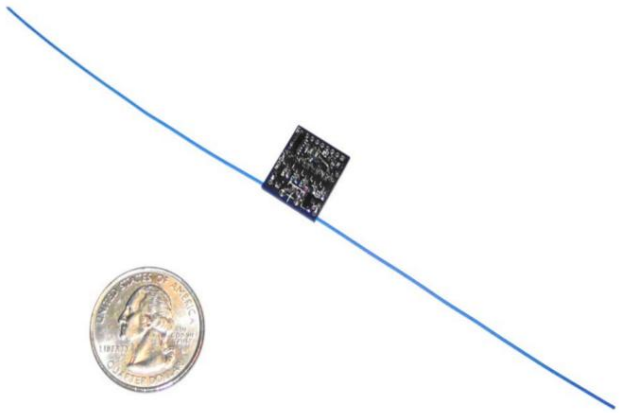


Abbildung 6: WISP

Solche Systeme wurden in Studien Motten eingesetzt um deren Nervensignale an den Flugmuskeln zu messen.

Das NeuralWISP kann somit von Neurowissenschaftlern eingesetzt werden um neurologische Signale aufzuzeichnen und die Spitzen des Signals an einen Computer zu übertragen. Dazu wird das System einem Tier implantiert und mit dessen Nervensträngen verbunden. Mikroelektronische Bauteile detektieren die gewünschten Nervensignale und leiten sie an eine RFID-Antenne wei-

ter, welche das Signal an das Lesegerät überträgt. Die Energie die das NeuralWISP benötigt wird durch RFID-Technik bereitgestellt. Der Strom wird von einer Funkquelle bezogen, welche bis zu einem Meter entfernt sein kann. Die Funkquelle ist ein handelsübliches RFID-Lesegerät. Dadurch kann das beispielsweise bei Mäusen implantierte System kabellos und ohne Batterie mit elektrischer Energie versorgt werden. Da auf ein Kabel verzichtet werden kann, verkleinert sich das Infektionsrisiko signifikant. Ein weiterer Vorteil ergibt sich durch den Verzicht auf eine Batterie, da diese gewechselt werden müsste was einen chirurgischen Eingriff erfordern würde.

Um das NeuralWISP mit einem passiven RFID-System betreiben zu können, muss aber extrem stromsparende Mikroelektronik eingesetzt werden. Entscheidend ist vor allem der programmierbare Mikrocontroller, der die gewünschten Signale aufzeichnet. [12]

3.2 Vor- / Nachteile

Nach längerer Betrachtung wurde klar, dass man die Vor- und Nachteile implantierter RFID-Chips bei jedem System einzeln beurteilen muss.

3.2.1 **Vorteile**:

Verwendet man die RFID-Technik wie im Beispiel des VeriChip lediglich zur Identifizierung und zum referenzieren auf persönliche Daten, ist es fraglich ob ein solcher Chip implantiert werden muss. Den gleichen Nutzen hätte man, wenn der Chip in einer Armbanduhr oder ähnliches eingebaut wäre. Natürlich käme in diesem Fall die Gefahr des Verlusts des RFID-Chips hinzu, ob das aber eine Implantation rechtfertigt ist Ansichtssache.

Betrachtet man das NeuralWISP so sind die Vorteile von RFID offensichtlicher. Da auf ein Kabel zur Stromversorgung des implantierten Systems verzichtet werden kann und somit kein dauerhafter transdermaler Anschluss vorhanden ist, verringert sich das Infektionsrisiko des Testobjekts. Des Weiteren kann auf chirurgische Eingriffe verzichtet werden, die bei einem NeuralWISP mit Batterie notwendig wären. Dadurch wird der Versuch massiv vereinfacht und auch das Tier kann geschont werden.

Diese Vorteile stehen in direktem Zusammenhang mit der verwendeten RFID-Technologie und wären ohne diese nicht gegeben.

3.2.2 Nachteile:

Die Nachteile die implantierte RFID-Chips haben, sind die Gefahren die bei allen Implantaten vorhanden sind und zusätzlich die Strahlenbelastung.

Bei einem undichten Implantat welches eine Kupferantenne enthält ist mit Entzündungen und Vergiftungen zu rechnen. Auch beim Implantieren ist ein geringes Risiko vorhanden. Ein Punkt ist die Sterilität, die bei allen subkutanen Injektionen notwendig ist. Logischerweise können implantierte RFID-Systeme nur durch einen chirurgischen Eingriff entfernt werden, was ebenfalls nachteilig sein kann.

Auf die weiteren Nachteile wie zum Beispiel das Krebsrisiko, wird im Teil *Gefahren und Risiken* vertieft eingegangen.

3.3 Zukünftige Entwicklungen

Mit dem NeuralWISP wurde schon eine Anwendung von RFID gezeigt, welche in Zukunft beispielsweise interessant für diagnostische Systeme sein kann.

Weitere Entwicklungen sind Nanoroboter. Dabei handelt es sich um Sensoren die in-vivo, also in lebenden Organismen, Messungen über Stoffkonzentrationen usw. durchführen. Solche Systeme würden bei der Therapie von Patienten mit Diabetes mellitus einen grossen Fortschritt bedeuten. Die benötigte Energie kann mit RFID kabellos dem implantierten Chip zu Verfügung gestellt werden. Zusätzlich könnte man den Datenverkehr zwischen Sensor und Auswertesystem durch RFID regeln.

3.3.1 Implantierter Glukose-Sensor und Nanoroboter:

Ein implantierbarer Glukose-Sensor wird unter anderem von der VeriChip Corp. entwickelt und soll die Diabetes-Therapie revolutionieren. Es handelt sich hierbei um ein völlig autonomes Messsystem welches in den Blutkreislauf injiziert wird und den Glukosegehalt misst.

In den letzten Jahren wurden schon mehrere Versuche unternommen ein solches System zu entwickeln, da es einerseits eine riesige Verbesserung der Therapie von Diabetes bedeuten würde, aber auch ökonomisch interessant wäre.

Zurzeit muss die Glukosekonzentration mit einer Blutprobe gemessen, was mehrmals am Tag einen kleinen Stich durch die Haut des Diabetikers erfordert. Dies wäre mit einem implantierten Sensor nicht mehr nötig, was ein grosser Mehrwert für den Patienten ist. An-

hand des Messwertes und je nach Ernährung entscheidet der Diabetiker wie viel Insulin er spritzt um die Blutzuckerkonzentration zu senken. Daran würde sich auch mit dem neuen System nichts ändern, da es lediglich ein Sensor ist und keine Möglichkeit zur Insulingabe vorhanden ist.

Bei der heutigen Insulin-Therapie entstehen fortlaufende Kosten, zum Beispiel durch den Einsatz von Einweg-Teststreifen. Diese wären mit einer in-vivo Messung natürlich nicht mehr nötig.

Bis man aber bei der Blutzuckermessung implantierte Sensoren einsetzt, braucht es noch einiges an Entwicklungsarbeit zu leisten. Das Projektteam um VeriChip Corp. nennt folgende Komponenten des Sensors als kritisch:

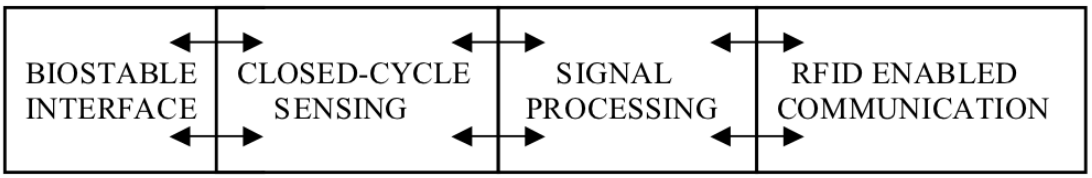


Abbildung 7: Kritische Komponenten

Zwar ist noch nichts von einem Prototyp des implantierbaren Glukose-Sensors bekannt, doch schematisch gibt es das Implantat schon.

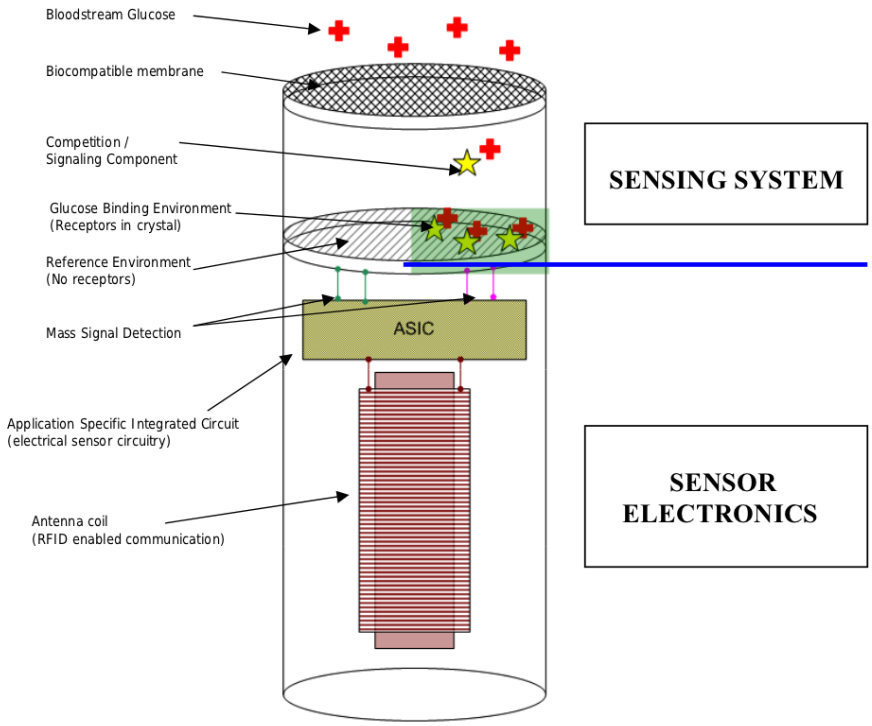


Abbildung 8: Schema Glucose-Sensor

Das Bauteil wird in Messsystem und Elektronik unterteilt. Ein Teil der Elektronik ist für die Übertragung der Messungen zuständig. Dies wird mit Hilfe einer RFID-Antenne gemacht, welche höchstwahrscheinlich auch die Energie die das System benötigt, bereitstellt. Die Energiezufuhr wird entweder durch Induktion oder mit Funkwellen gemacht. Wie das genau geschieht kann in den *Grundlagen der RFID-Technologie* nachgelesen werden.

Natürlich sind auch andere in-vivo Diagnostiksysteme denkbar, so zum Beispiel der Blutdruck. Solche Systeme werden als Nanoroboter bezeichnet und könnten in Zukunft bei der permanenten Patientenüberwachung eingesetzt werden. Um die Handhabung dieser Sensoren zu erleichtern, ist die Verknüpfung mit Mobiltelefonen sehr sinnvoll und wurde auch schon in Studien behandelt. [13][14]

3.4 Gefahren und Risiken

Hier werden die gesundheitlichen Gefahren erläutert die von implantierten RFID-Chips ausgehen können. Die gesellschaftlichen Risiken sind im letzten Kapitel ausgeführt.

Der grösste gesundheitliche Schaden wird beim Krebsrisiko angenommen. Eine Mehrheit von unabhängigen Studien kommt zum Schluss, dass aufgrund eines implantierten Mikrochips vermehrt Krebszellen gebildet werden.

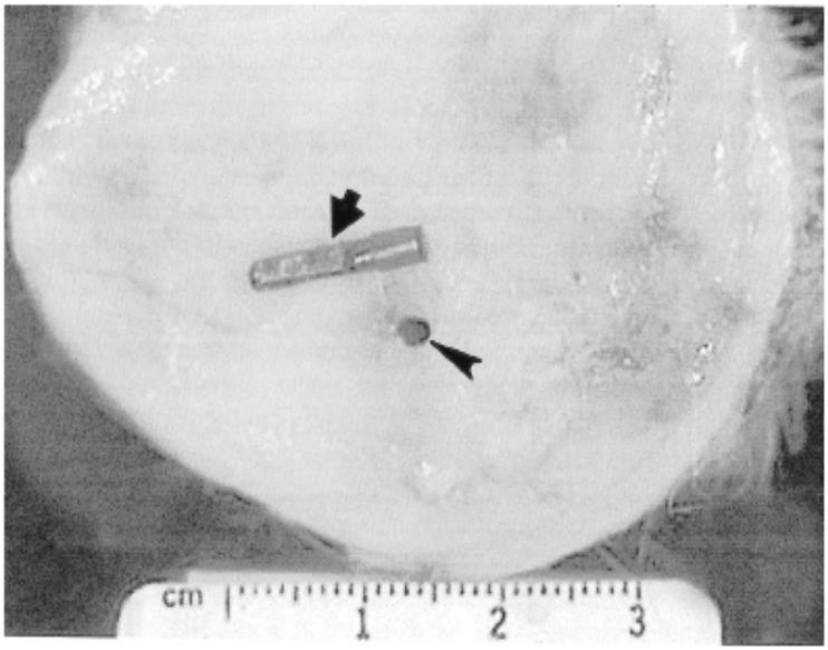


Abbildung 9: Krebszelle neben RFID-Chip

Es wurden 4 Gründe für die Tumorbildung in Zusammenhang mit implantierten Mikrochips ermittelt:

- **Fremdkörperbedingte Tumorbildung:**

  Der Mikrochip wird subkutan implantiert und vom Körpergewebe als Fremdkörper erkannt. Dadurch kann die Kommunikation zwischen den Zellen gestört werden und es zur Bildung von Tumoren kommen.

- **Post-Injektionale Tumorbildung:**

  Nach der Injektion kann es in der Umgebung des Chips zu Entzündungen kommen, welche auch zu Krebs führen kann.

- **Mögliche Genotoxizität des Implantats:**

  Wenn die Implantat Hülle mit genotoxischen Stoffen belastet ist, kann es zur Krebsbildung kommen.

- **Elektromagnetische Strahlung von Chip und Lesegerät:**

  Krebsbildung aufgrund der Funkwellen die ausgestrahlt werden.

Da diese Beobachtungen bei Tieren, vor allem Hunden, gemacht wurden kann man nicht mit absoluter Sicherheit sagen, dass auch beim Mensch ein erhöhtes Krebsrisiko vorhanden ist. Über Langzeiteffekte von RFID-Chips die in Menschen implantiert wurden, ist nur sehr wenig bekannt. Dies ist auch ein Punkt den Chip-Kritiker bemängeln und konkrete Massnahmen fordern:

- Keine weiteren Implantationen von RFID-Chip in Menschen
- Personen die bereits einen Chip implantiert haben, über die Risiken informieren und eine Entfernung anbieten.
- Sollte sich eine Person entschliessen den Chip zu behalten, so sollen regelmässige Untersuchung zu Auswirkungen des Chips auf den Menschen gemacht werden.
- Regulierungen zur weiteren RFID-Forschung sollen eingeführt werden. [15]

4 Datenschutz und Privatsphäre

Abbildung 10: Datenschutz

Wir leben in einer Zeit in der immer mehr Informationen anfallen, die durch neue Informationstechnologien immer effizienter und in grösseren Mengen gespeichert werden können, wie z. B. die RFID-Technologie.

Dadurch entstehen jedoch diverse Datenschutzrechtliche Probleme, und es werden gesetzliche Bestimmungen benötigt um heikle Personendaten (Name, Wohnort, Alter etc.) zu schützen und Massnahem daraus abzuleiten.

RFID-Anwendungen werden aus Datenschutzrechtlicher Sicht problematisch, wenn damit Personendaten bearbeitet werden. [16]

4.1 Rechtliche Grundlagen Schweiz

In der Schweiz ist der Datenschutz seit dem 1.Juli 1993 im Bundesgesetz über den Datenschutz (DSG) geregelt. Wenn Personendaten bearbeitet werden, kommt das darin enthaltene „Grundrecht zur informationellen Selbstbestimmung“ zur Geltung.
Es legt, wie aus dem Namen ersichtlich, vor allem Wert auf die Möglichkeit zur Selbstbetimmung von Personen.
Implantierte RFID-Chips sind deshalb problematisch, weil dadurch direkte Rückschlüsse auf die betroffene Person gemacht werden können. Aber auch bei RFID-Armbändern, wie sie z. B. bei Patienten im Spital Thun verwendet werden, liegt die gleiche Problematik vor. Weiter sind alle Anwendungen aus Datenschutzrechtlicher Sicht bedenklich, mit denen indirekt auf Personen geschlossen werden kann, wie z. B.: Ticket, Kleidungsstück, Skipass, Kundenkarte etc. [16]

4.2 Rechtliche Grundlagen EU

In der EU gilt bezüglich Datenschutz die im Jahr 1995 erlassene „Richtlinie 95/46/EG (Datenschutzrichtlinie)“. Sie regelt ähnlich wie in der Schweiz den Umgang mit heiklen Personendaten. Darin werden die Mindeststandarts für die Mitglieder der EU vorgegeben.

Bezüglich RFID-Chips wurde anfangs April 2011 eine neue Leitlinie verabschiedet, die die Datenschutzrisiken in allen Bereichen minimieren soll, in denen RFID-Chips Anwendung finden, z. B. im Gesundheitswesen oder im Einzelhandel. Die Leitlinie behandelt vor allem die Abklärung aus Datenschutzrechtlicher Sicht bevor ein RFID-basiertes Produkt auf den Markt gebracht wird. Fällt die Abklärung negativ aus, müssen entsprechende Massnahmen getroffen werden.

Ein Hauptgrund für die neue Richtlinie ist, dass der Anteil der EU am internationalen RFID-Chipmarkt vermutlich in Zukunft stetig ansteigen wird. Die EU-Kommissarin für Informationsgesellschaft und Medien schätzt, dass der Anteil in den nächsten 8 Jahren auf bis zu 35 % ansteigen könnte. [17] [18] [19]

4.3 Probleme

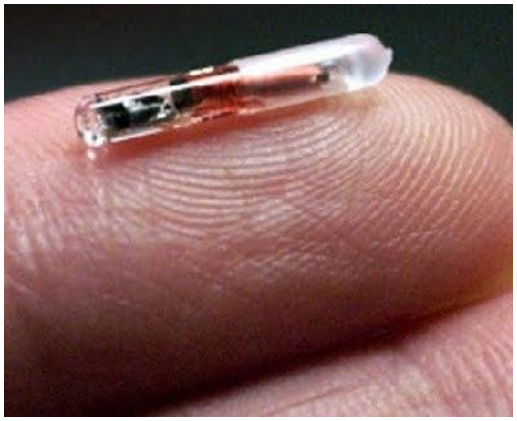


Abbildung 11: RFID-Tag

Die Datenschutzrechtlichen Probleme die sich aus der Nutzung der RFID-Technologie ergeben sind vielschichtig, deshalb kann keine allgemeine Beurteilung vorgenommen werden. Bei der Beurteilung muss jeweils auf den spezifischen Anwendungsfall geschaut werden. Basierend auf dem Bericht des Bundes: „Handlungsbedarf im Zusammenhang mit RFID-Technologie“, können jedoch 4 Grundsätzliche Probleme abgeleitet werden:

- **Kleinheit von RFID-Tags**
  Durch die geringe Grösse der RFID-Tags ist es möglich, dass diese verdeckt und für die betreffende Person nicht erkennbar dieser zugeführt werden. Z. B. eingenäht in Kleidungsstücke, oder im Geldbeutel. Weiter könnten diese auch in Teppiche etc. eingenäht/angebracht werden.

- **Verwendung drahtloser Funktechnologie**
  Durch die Verwendung drahtloser Funktechnologie ist es möglich, dass diese aus bis zu mehreren Metern ausgelesen werden können, ohne dass dies für die betreffende Person erkennbar ist.

- **Datenspeicherung**
  Die Daten, die auf RFID-Chips gespeichert werden fallen kontinuierlich an, und nicht nur bei „Bedarf“ wie z. B. bei Barcodes. Somit hat der Nutzer keine Kontrolle über den Erfassungsvorgang. Solange die Chips nicht zerstört oder deaktiviert werden, können diese weiter ausgelesen werden.

- **Verwendungsart**
  Auch bei Anwendungen, die nicht direkt auf das Erfassen von Personendaten ausgelegt sind, z.B. Waren, Kleidungsstücke, Banknoten etc., könnten anfallende Randdaten dennoch zur Lokalisation oder Identifizierung von Personen verwendet werden. [16] [20]

4.4 Massnahmen

Ebenfalls auf dem oben genannten Bericht des Bundes können diverse Massnahmen abgeleitet werden, um die Risiken in Bezug auf den Datenschutz einzugrenzen:
Personen müssen umfassend über die technischen Möglichkeiten von RFID-System informiert werden. Im Internet kann sich zudem leicht jeder selber informieren. Eine gute Seite zu diesem Thema ist: http://rfid-informationen.de/
Wenn durch RFID-Tags Kommunikationsvorgänge stattfinden, bei denen Personendaten bearbeitet werden, muss dies für die betroffene Person klar und eindeutig erkennbar sein.
Daten dürfen nicht länger gespeichert werden, als dies für die jeweilige Anwendung erforderlich ist.

Es muss möglich sein, gespeicherte Daten jederzeit zu löschen.

Die Sicherheit der Daten muss gewährleistet sein. Dieser, aus unserer Sicht wichtigster Punkt kann durch diverse Massnahmen gewährleistet werden:

Eine Passwort-Authentifizierung zwischen RFID-Tag und Lesegerät.

Eine Verschlüsselung der Daten durch das so genannte „Hash-Lock"-Verfahren.

Blocker-Tags, die das unerlaubte Auslesen von Daten verhindern

Eine durch den so bezeichneten „Kill-Befehl" ausgelöste Deaktivierung der spezifischen Seriennummer eines RFID-Tags, so dass diese nicht mehr ausgelesen werden kann. [16] [21]

4.5 Gesellschaftliche Akzeptanz

Abbildung 12: Biometriezwang

Die Einstellung der Bevölkerung zu RFID-System ist ambivalent. Einerseits werden gewisse Anwendungen befürwortet, wie z.B. die obligatorische Implantierung eines RFID-Chips bei Hundewelpen, und andere werden mit Misstrauen betrachtet, so z.B. die für Menschen als erste kommerziell erhältliche, implantierbare Version namens „VeriChip".

Ein aktuelles Beispiel, das die Problematik gut aufzeigt, ist die Abstimmung über Biometrische Pässe vom 17 Mai 2009, die ja bekanntlich historisch knapp angenommen wurde.

- **Argumente der Befürworter**

  Die Vorlage wurde vor allem von der bürgerlichen Seite gutgeheissen. Sie befürchteten bei einer Ablehnung, dass der Wirtschafts- und Tourismusstandort Schweiz gefährdet sei. Ausserdem würden Biometrische Pässe für Reisen in die USA ohne Visum benötigt. Durch die Verschlüsselung der RFID-Daten sahen sie die Datensicherheit nicht gefährdet.

- **Argumente der Gegner**

  Die Gegner der Vorlage stammten hauptsächlich aus Linken Kreisen. Sie befürchteten erhöhte Sicherheitsrisiken bezüglich der zentralen Speicherung der Daten. Bezogen auf RFID-Chips bemängelten Sie, dass diese von Dritten unrechtmässig ausgelesen werden könnten.

  Bestätigt wurde diese Befürchtung, als vor ca. 5 Jahren in den Niederlanden erfolgreich ein Biometrischer Pass geknackt wurde. Der holländische Sicherheitsspezialist Riscure aus Delft erläuterte, dass es möglich sei, den Pass innert 2 Stunden und mit einem Abstand von bis zu 10 Metern zwischen RFID-Chip und Lesegerät auszulesen. Die Sicherheit von sensiblen Personendaten wäre somit nicht mehr gewährleistet. [22] [23]

5 Fazit

Die RFID-Technologie ist sicher eine Technologie, die in Zukunft mehr und mehr an Bedeutung gewinnen wird. Die Technologische Entwicklung wird allgemein im Bereich der Mikro- und Nanotechnologie mehr und mehr beschleunigt. Es wird geschätzt, dass der Anteil Europas am globalen Markt in den nächsten 8 Jahren auf bis zu 35 % ansteigen wird.
Darin liegt einerseits ein grosses Potential, so z. B in der Tieridentifikation, Verpackungsindustrie, Krankenhäuser etc.
Andererseits gibt es aber auch Bedenken in gewissen Bereichen, so z.B. bei Biometrischen Pässen, oder auch bei immer häufiger Vorkommenden, bei Menschen implantierbaren RFID-Chips.
Es wird deshalb nötig sein, nationale und grenzüberschreitende Regulierungen und Normierungen zu schaffen und weiter auszubauen, um das persönliche Grundrecht auf Datenintegrität zu gewährleisten.
Wir hoffen, dass wir mit unserer Arbeit einen guten Überblick über die Thematik aufzeigen konnten.

6 Quellen und Abbildungsverzeichnis

6.1 Quellenverzeichnis

Nummer	Quelle
1	http://de.wikipedia.org/wiki/RFID [Stand: 01.06.11]
2	http://de.wikibooks.org/wiki/RFID-Technologie [Stand: 01.06.11]
3	http://en.wikipedia.org/wiki/Microchip_implant_(human) [Stand: 01.06.11]
4	http://www.medien.ifi.lmu.de/lehre/ws0607/mmi1/essays/Sebastian-Loehmann.xhtml [Stand: 01.06.11]
5	http://medienwissenschaft.uni-bayreuth.de/dimensionen/unterrichtsentwuerfe/Unterrichtsentwurf_RFID-Technik.pdf [Stand: 01.06.11]
6	http://www.anis.ch/de/microchip/ [Stand: 25.05.11]
7	http://www.wikipedia.org/wiki/VeriChip [Stand: 25.05.11]
8	http://www.heise.de/tr/artikel/Der-Chip-der-unter-die-Haut-ging-836048.html [Stand: 25.05.11]
9	http://www.verimedinfo.com/for_patients.asp [Stand: 26.05.11]
10	http://www.verimedinfo.com/for_physicians.asp [Stand: 26.05.11]
11	http://www.verimedinfo.com/for_med_fac.asp [Stand: 26.05.11]
12	http://web.media.mit.edu/~jrs/neuralwisp.pdf [PDF] [Stand: 28.05.11]
13	http://www.positiveidcorp.com/glucose_sensing.html [Stand: 28.05.11]
14	http://www.sciencedirect.com/science/article/pii/S1549963408000348 [PDF] [Stand: 25.05.11]
15	http://www.antichips.com/cancer/index.html [Stand: 29.05.11]
16	http://www.edoeb.admin.ch/dokumentation/00445/00472/00576/index.html?lang=de [Stand: 03.06.11]
17	http://de.wikipedia.org/wiki/Richtlinie_95/46/EG_%28Datenschutzrichtlinie%29 [Stand: 03.06.11]
18	http://www.computerbase.de/news/internet/webweites/2011/april/eu-leitlinienabkommen-fuer-rfid-datenschutz-steht/ [Stand: 03.06.11]
19	http://www.zdnet.de/news/wirtschaft_telekommunikation_eu_erlaesst_datenschutzrichtlinie_fuer_rfid_story-39001023-41004021-1.htm [Stand: 03.06.11]
20	http://epic.hpi.uni-potsdam.de/pub/Home/SensorNetworksAndIntelligentObjects2007/MS07_-_Management_von_RFID-Daten.pdf [Stand: 03.06.11]

21	http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate 19060/ppdatenschutz.pp.funpic.de/joomla_test/index2ea28.pdf [Stand: 27.05.11]
22	http://www.vimentis.ch/publikation/151/Abstimmung+17.+Mai+2009:+Biometrische+P%E4sse.html [Stand: 27.05.11]
23	http://www.heise.de/tp/artikel/21/21907/1.html [Stand: 27.05.11]

6.2 Abbildungsverzeichnis

Nummer	Abbildungsname & Quelle
1	Britisches Radar im 2. Weltkrieg http://www.ozatwar.com/raaf/shepherdshillradar01.jpg
2	RFID-Frequenzen http://talbros.net/images/RFID_Passive.gif
3	RFID-Tag http://www.trade-and-service.de/media/RFID-Chip.jpg
4	Spezialspritze http://www.Wikipedia.org/wiki/Tierkennzeichnung
5	VeriChip http://daysaheadnews.com/health/verichips_hidden_costs.html
6	WISP http://web.media.mit.edu/~jrs/neuralwisp.pdf
7	Kritische Komponenten http://www.positiveidcorp.com/glucose_sensing.html
8	Schema Glucose-Sensor http://www.positiveidcorp.com/glucose_sensing.html
9	Krebszelle neben RFID-Chip http://www.antichips.com/cancer/index.html
10	Datenschutz http://www.presseverein.ch/2009/06/vorsicht-mit-personlichen-daten/
11	RFID-Tag http://conspiracies.co.ohost.de/?p=421
12	Biometriezwang http://blog.ich-wars-nicht.ch/2009/02/nein-zum-biometriezwang/