

Batteriegestützte Transponder in ISO/IEC 14443. Eine neue Transponder-Klasse

Klaus Finkenzeller

Giesecke & Devrient, Prinzregentenstraße 159
81607 München
Klaus.Finkenzeller@gi-de.com

Zusammenfassung

Ursprünglich für kontaktlose Chipkarten im Formfaktor ID1 entwickelt, findet die ISO/IEC 14443 in immer unterschiedlicheren Formfaktoren neue Anwendungen. Am bekanntesten unter den neuen „Bauformen“ sind dabei Anwendungen wie der elektronische Reisepass ePass, oder kontaktlose Kreditkarten in einem Format, das nur mehr halb oder ein Drittel so groß wie ID1 ist. Gerade der Drang zu immer kleineren Formfaktoren führt jedoch immer häufiger zu Problemen im Feld, da die kleinen Transponder nicht immer sicher ausgelesen werden können. Problematisch wird es, wenn die kontaktlosen Datenträger noch weiter miniaturisiert werden und zum Beispiel als micro-SD oder SIM-Karte in einem Mobiltelefon eingebaut betrieben werden, da hier eine zuverlässige Kommunikation mit dem Lesegerät nicht mehr gewährleistet werden kann. Abhilfe schafft nun ein neuer Vorschlag in der Standardisierung, welcher den Einsatz batteriegestützter Transponder beschreibt. Der folgende Artikel beschreibt die physikalischen Grundlagen dieser Transponder, sowie das weitere Vorgehen in der Standardisierung.

1 Einführung

Der Grundstein der Norm für kontaktlose Chipkarten, ISO/IEC 14443 wurde bereits 1993 mit einem New Work Item (NWI) „Remote Coupling Communication Cards“ [WG8N0165] gelegt. In den folgenden 7 Jahren entstand ein Standard, der heute in Zig-Millionen kontaktlosen Datenträgern überall auf der Welt eingesetzt wird und damit der wohl erfolgreichste RFID-Standard überhaupt ist. Zu den klassischen Anwendungen zählten Ticketing im öffentlichen Nahverkehr, Zutritt zu Gebäuden oder der bargeldlose Zahlungsverkehr. Ab dem Jahr 2000 kamen weitere Anwendungen wie etwa der elektronische Reisepass (ePass), kontaktlose Kreditkarten und zuletzt der neue deutsche Personalausweis (nPA, vormals ePA) [BMI_10].

Technisch gesehen spezifiziert die ISO/IEC 14443 ein induktiv gekoppeltes RFID-System [Fink08], so wie auch Systeme nach ISO/IEC 15693 (Vicinity Karte, z. B. für Ski-Pässe), ISO/IEC 18000-3 (Waren- und Güterlogistik) oder ISO/IEC 18092 (Near Field Communication). Zur Energieversorgung der Datenträger (Transponder) sowie zur Datenübertragung vom Leser zum Transponder erzeugen die Lesegeräte induktiv gekoppelter RFID-Systeme ein starkes, hochfrequentes magnetisches Wechselfeld im Frequenzbereich 13,56 MHz. Gelangt

ein passiver (batterieloser) Transponder in das magnetische Feld eines Lesegerätes so wird er durch die in der Antennenspule induzierte Spannung mit Energie zum Betrieb versorgt. Zur Datenübertragung vom Lesegerät zur kontaktlosen Chipkarte wird in der Regel die Amplitude des magnetischen Wechselfeldes moduliert. Bei ISO/IEC 14443 eingesetzte Modulationsverfahren sind z. B. ASK 100% (Typ A) oder ASK 10% (Typ B).

Die physikalischen Parameter der ISO/IEC 14443 sind nun so definiert, dass sich bei hohen Bitraten (106 .. 868 kBit/s), hohem Energieverbrauch des Transponderchips (Mikroprozessor mit Smart Card Betriebssystem) und der Chipkarten-Bauform ID1 eine typische Lesereichweite von 10 cm oder weniger ergibt.

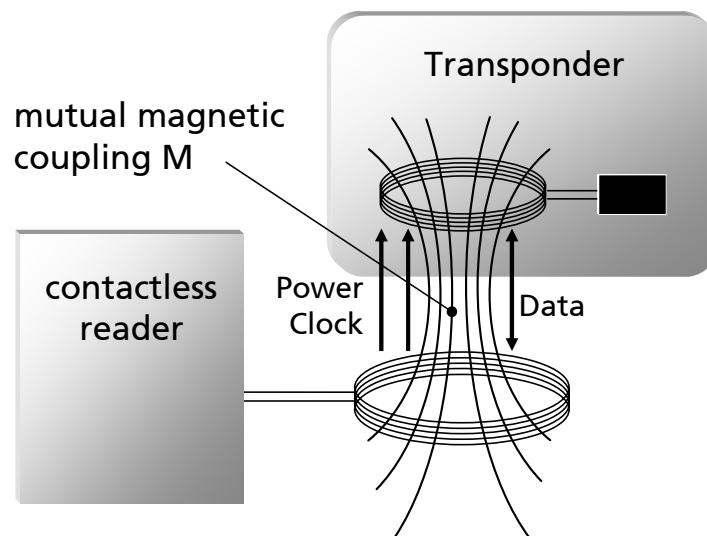


Abbildung 1: Grundsätzlicher Aufbau eines induktiv gekoppelten Transpondersystems

Zur Datenübertragung vom Transponder zum Lesegerät wird eine **Lastmodulation** eingesetzt. Hierbei wird ein der Antenne des Transponders parallel geschalteter Lastwiderstand im Takt des zu übertragenden Signals ein- und ausgeschaltet. Bei der ISO/IEC 14443 wird der Lastmodulator durch einen modulierten Hilfsträger (848 kHz) getastet. Das Ein- und Ausschalten des Lastwiderstands bewirkt eine sprunghafte Veränderung des Stromes in der Transponderantenne und damit einhergehend eine Veränderung in der Rückwirkung der Transponderantenne auf die Amplitude des Magnetfelds des Lesegerätes („Transformatorprinzip“). Diese durch die Lastmodulation bewirkte Amplitudenmodulation des Magnetfelds kann durch das Lesegerät einfach detektiert werden [Fink08].

Die begrenzenden Faktoren eines solchen induktiv gekoppelten RFID-Systems hinsichtlich der Kommunikationsreichweite liegen dabei einerseits in der Energiereichweite des Lesegerätes, also der Fähigkeit einen Transponder im Leseabstand mit ausreichend Energie zum Betrieb zu versorgen, sowie andererseits in der Fähigkeit Daten per Lastmodulation vom Transponder an das Lesegerät zurückzusenden. In beiden Fällen wird eine ausreichende große magnetische Gegenkopplung (*mutual magnetic coupling M*) zwischen der Antenne des Lesegerätes und der Antenne des Transponders benötigt. Mit kontaktlosen Chipkarten im typischen Format ID1 ist diese Bedingung innerhalb der typischen Lesereichweite von 10 cm erfüllt. Werden hingegen sehr kleine Antennen im Formfaktor einer SIM-Karte oder einer micro-SD Karte eingesetzt, so sinkt die magnetische Gegenkopplung und damit die erreichbare Lesereichweite drastisch ab. Soll eine solche kleine kontaktlose Karte beispielsweise in ein

Mobiltelefon oder in ein PDA eingesetzt werden um diese mit einem kontaktlosen Interface auszustatten, so führt die kleine Lesereichweite von evtl. nur wenigen Zentimetern schnell zu einem Problem, insbesondere wenn die Karte bei zusätzlich auftretender Abschirmung (z.B. durch den Akku) schließlich nicht mehr in der Lage ist die Reichweite zu einem außerhalb befindlichen Lesegerät zu überbrücken.

In diesem Artikel wird gezeigt wie sich die Reichweitenlimitierung eines induktiv gekoppelten RFID-Systems mit sehr kleinen Antennen durch den Einsatz eines aktiven, batteriegestützten Transpondersystems umgehen lässt.

2 Funktionsweise aktiver Transponder

Um auch mit Transpondern mit sehr kleiner Antennengeometrie akzeptable Lesereichweiten zu erzielen, müssen die vorher beschriebenen begrenzenden Faktoren beseitigt werden. Wir unterscheiden dabei zwischen der Übertragungsrichtung vom Lesegerät zum Transponder (Downlink) und der umgekehrten Richtung (Uplink).

2.1 Downlink

Im Falle der Energiereichweite ist das Problem einer zu geringen magnetischen Gegenkopplung einfach zu lösen. Hierzu ist es lediglich notwendig den Transponder aus einer lokalen Energiequelle (Batterie) mit Strom zu versorgen. Wird der Transponder in der Bauform einer SIM-Karte oder einer micro-SD Karte im Mobiltelefon betrieben, so wird die Energie über einen Anschlusspin vom Mobiltelefon zur Verfügung gestellt.

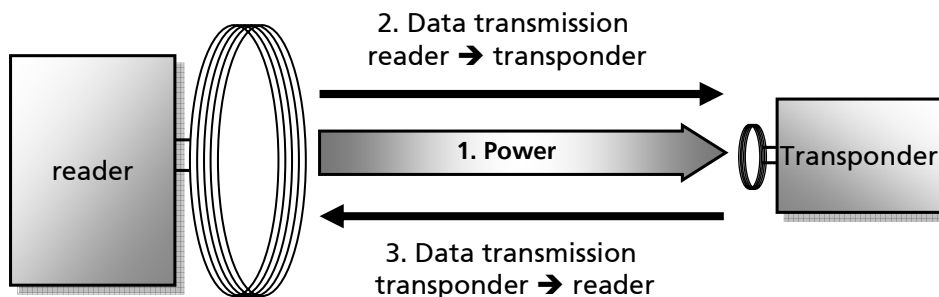


Abbildung 2: Die die Lesereichweite begrenzenden Faktoren eines induktiv gekoppelten RFID-Systems.

Um einen Transponder mit Energie zu versorgen, müsste eine Spannung von wenigstens 3 V in der Transponderantenne induziert werden. Bei einem batteriegestützten Transponder hingegen wird die in der Antenne induzierte Spannung nicht mehr zur Energieversorgung verwendet, sondern nur noch dazu, Daten und Kommandos vom Lesegerät zu empfangen. Hierzu reicht aber eine Spannung mit erheblich geringerem Pegel von wenigstens einigen mV bereits aus, da diese einfach verstärkt werden kann. Auf diese Weise kann das Signal des Lesegeräts auch mit kleinsten Transponderantennen und Metallabschirmung auf deutliche größere Entfernung detektiert werden.

2.2 Uplink

Etwas komplexer ist die Optimierung der Datenübertragung vom Transponder zurück zu einem Lesegerät. Die üblicherweise verwendete (passive) Lastmodulation scheidet auch bei einem Transponder mit externer Energieversorgung (aktiver Transponder) aus, da sich ohne eine Verbesserung der magnetischen Kopplung nur eine unwesentliche Verbesserung gegenüber einem passiven (batterielosen) Transponder ergibt. Eine Vergrößerung der magnetischen Kopplung wäre aber nur durch eine Verringerung des Abstands zwischen den Antennen (sofern noch möglich) und einer Vergrößerung der Antennenfläche des Transponders möglich. Die Vergrößerung der Antennenfläche bedingt jedoch eine entsprechend größere Bauform des Transponders und scheidet somit für uns aus.

Eine Alternative besteht darin, auf anderem Wege ein Signal zu erzeugen, welches im Frequenzspektrum dem Signal einer passiven Lastmodulation gleicht und dieses aktiv (d.h. unter Aufwendung von eigener Energie) an das Lesegerät zu senden. Ein solches Verfahren wird als aktive Lastmodulation (auch *enhanced modulation*) bezeichnet und nachfolgend genauer beschrieben.

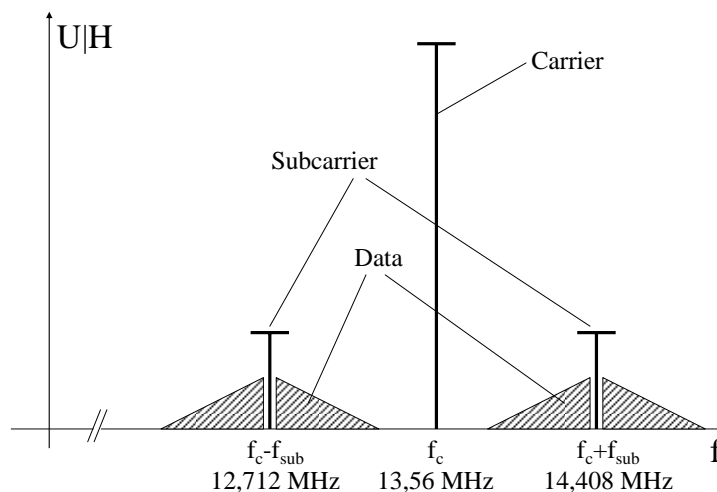


Abbildung 3: Ein durch Lastmodulation mit Hilfsträger entstandenes Frequenzspektrum an der Antenne eines Lesegerätes nach ISO/IEC 14443 [Fink08].

Betrachten wir das durch eine (passive) Lastmodulation an der Antenne des Lesegerätes auftretende Frequenzspektrum (vgl. **Abbildung 3**), so sind z.B. bei ISO/IEC 14443 neben dem Trägersignal (13,56 MHz) im Abstand der Hilfsträgerfrequenz (848 kHz) zwei weitere Spektrellinien (14,408 MHz und 12,712 MHz) zu erkennen, um die sich jeweils zwei Modulationsseitenbänderausbilden. Die Nutzdaten sind dabei ausschließlich in den Modulationsseitenbändern um die Hilfsträgerlinien enthalten.

Um Daten von einem aktiven Transponder an ein Lesegerät zu senden würde es ausreichen die beiden Hilfsträger-Spektrellinien mit den datentragenden Seitenbändern zu erzeugen und an ein Lesegerät zu senden. Das Trägersignal muss dabei nicht übertragen werden; dieses wird vom Lesegerät ohnehin permanent ausgesendet. Ein solches Signal wird als „Dual-Side-Band“ (DSB) Modulation bezeichnet.

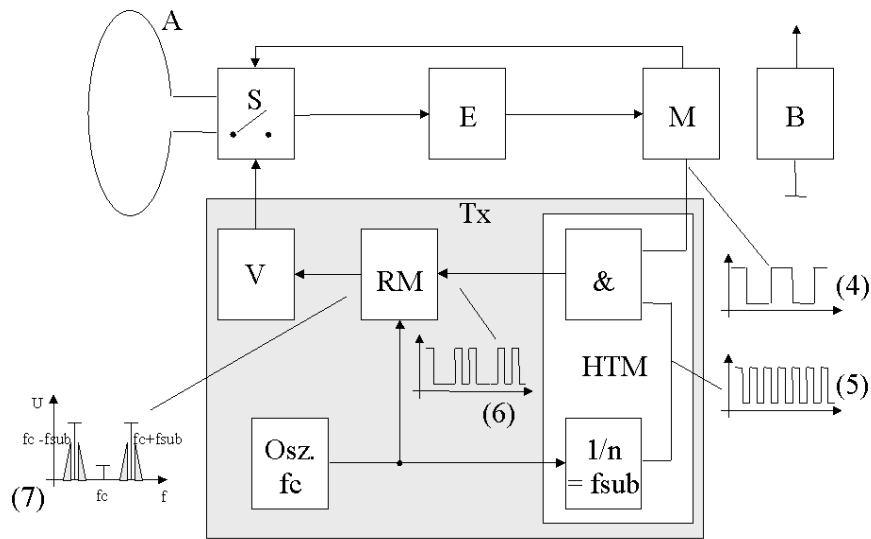


Abbildung 4: Das Blockschaltbild eines aktiven Transponders für ISO/IEC 14443
 (4 = Modulationssignal, 5 = Hilfsträger, 6 = Hilfsträger moduliert, 7 = DSB Signal)

Eine Grundschialtung der Nachrichtentechnik, mit der eine solche DSB-Modulation erzeugt werden kann, ist der Ringmodulator (RM). Der Ringmodulator wird mit einer Referenzfrequenz $f_c = 13,56 \text{ MHz}$ und dem modulierten Hilfsträger (6) gespeist. Das Ausgangssignal (7) des Ringmodulators ist dann bereits das benötigte DSB-Signal. Dieses wird in einem Verstärker (V) im Pegel angehoben und über die Antenne (A) abgestrahlt.

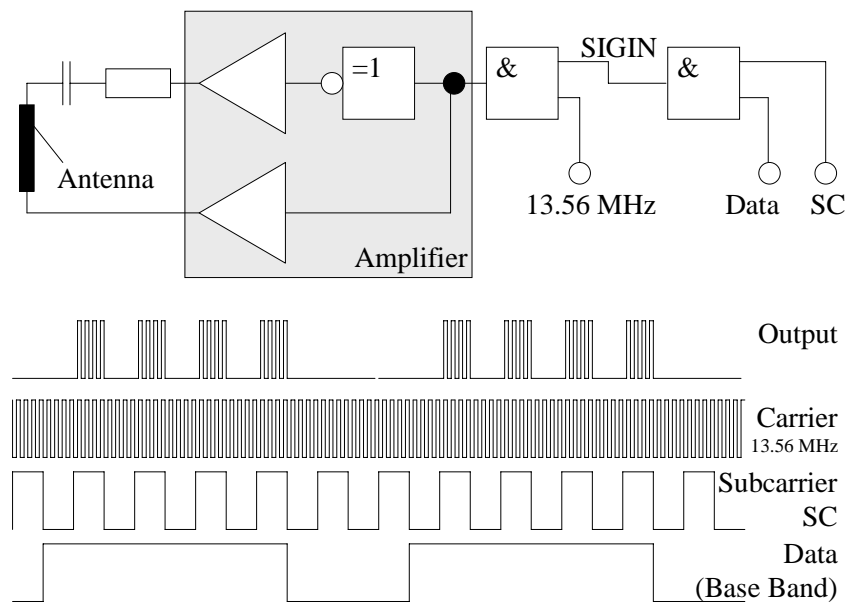


Abbildung 5: Die Erzeugung einer aktiven Lastmodulation mit einem einfachen ASK-Modulator

Da es sich bei den verfügbaren Signalen nicht um analoge, sondern um binäre Signale (Zustände high / low) handelt, können die benötigten Modulationsseitenbänder noch wesentlich einfacher durch eine Amplitudenmodulation erzeugt werden. Eine Amplitudenmodulation entsteht bei analogen Signalen wie bekannt durch die Multiplikation zweier Sinusschwingungen unterschiedlicher Frequenz:

$$U_{\text{mod}} = U_1 \cdot \sin(\omega_1 \cdot t) \cdot U_2 \cdot \sin(\omega_2 \cdot t)$$

Eine Multiplikation von Binärsignalen, also eine (2-)ASK-Modulation (*ASK = Amplitude Shift Keying*) kann durch eine einfache UND-Verknüpfung realisiert werden.

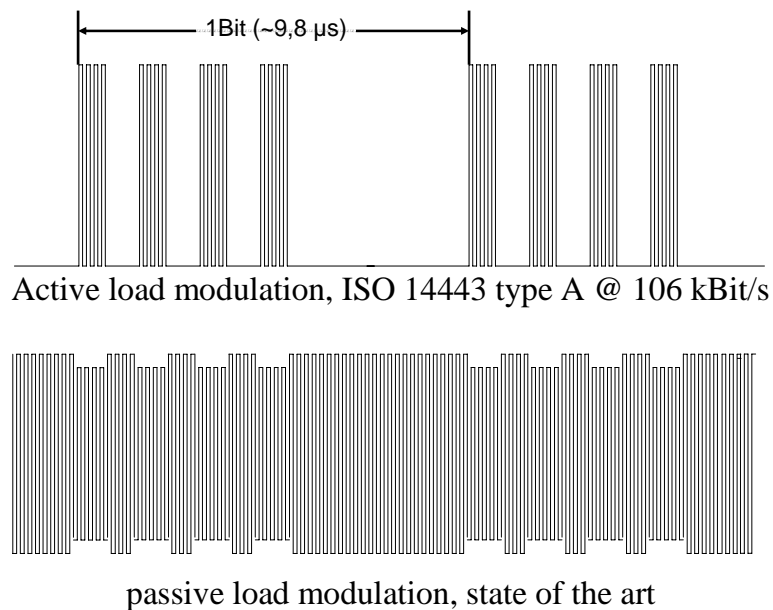


Abbildung 6: Vergleich der Signale einer aktiven und passiven Lastmodulation im Zeitbereich an der Antenne des Transponders.

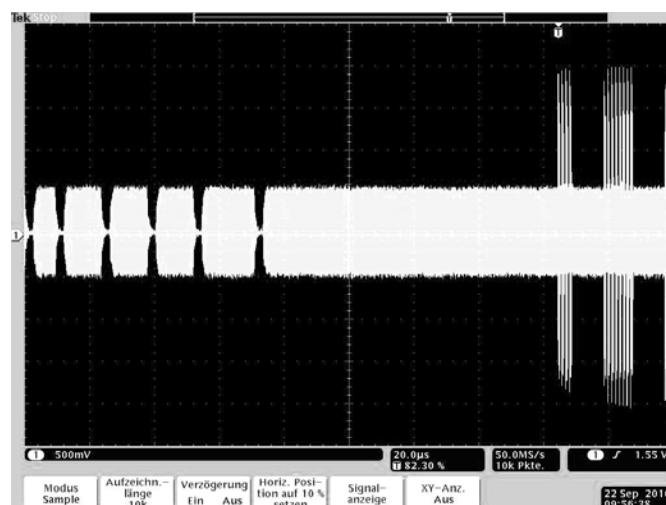


Abbildung 7: Spannungsverlauf in einer Messantenne (sense coil) während einer Datenkommunikation mit aktiver Lastmodulation. Links im Bild: Kommando eines Lesegeräts (Downlink, 100% ASK), Rechts im Bild: Antwort eines aktiven Transponders (Uplink)

Der passive Lastmodulator eines ISO/IEC 14443 Typ A Transponders wird mit einem durch einen Manchestercode modulierten Hilfsträgersignal angesteuert. Diese Ansteuerung führt beim aktiven Transponder mit ASK-Modulator zu einem Signal, welches aus jeweils vier Träger-Bursts pro Bit besteht und genau die gewünschten Modulationsseitenbänder erzeugt, wie sie in **Abbildung 3** dargestellt sind. Lediglich der 13,56 MHz Träger kann durch die ASK-Modulation nicht unterdrückt werden, was aber die Datenübertragung vom Transponder zum Lesegerät nicht weiter beeinflusst.

2.3 Einfluss der Antennengröße

Der Einfluss der Antennengröße eines aktiven Transponders auf die Lesereichweite wurde von uns empirisch ermittelt. Die Messungen erfolgten mit einem handelsüblichen Lesegerät nach ISO/IEC 14443.

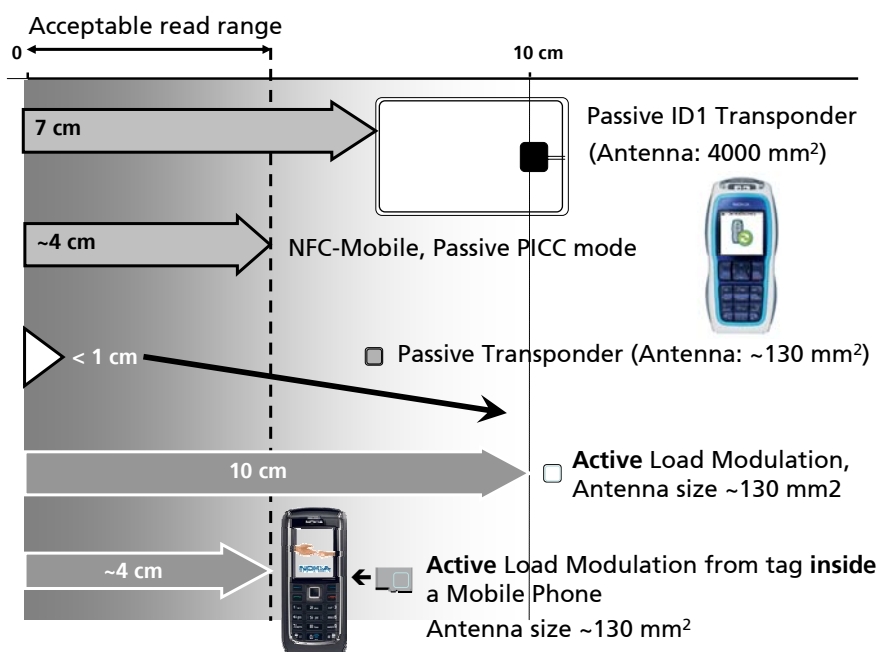


Abbildung 8: Die Reichweitenunterschiede zwischen aktiven und passiven Systemen bei unterschiedlicher Antennengröße.

Eine typische passive kontaktlose Chipkarte im ID1 Format konnte mit dem exemplarisch verwendeten Lesegerät über eine Entfernung von etwa 7 cm ausgelesen werden. Ein NFC-fähiges Mobiltelefon wurde in der NFC-Betriebsart „card emulation“ über eine Entfernung von etwa 4 cm ausgelesen. Wird die Antennenfläche des Transponders auf 130 mm², was der der typischen Fläche einer micro-SD Karte entspricht, verkleinert, so sinkt die Lesereichweite auf unter einen Zentimeter. Der Transponder muss auf das Lesegerät gelegt werden oder kann unter Umständen gar nicht gelesen werden. Wird solch ein kleiner Transponder in einem Gerät verbaut, z. B. einem Mobiltelefon, so wird durch die zusätzliche Metallabschirmung ein Auslesen fast unmöglich gemacht.

Unter Verwendung aktiver Lastmodulation war es hingegen möglich, den kleinen Transponder auf eine Entfernung von sogar 10 cm auszulesen – weit mehr, als die Lesereichweite einer

passiven kontaktlosen Chipkarte im ID1 Format. Selbst im eingebauten Zustand in einem Mobiltelefon können noch einige Zentimeter Lesereichweite erreicht werden.

3 Anwendungsbeispiel: Kontaktlose micro-SD Karte

Eine genauere Betrachtung des Marktes für Mobiltelefone lässt darauf zurückschließen, dass der Anteil NFC-fähiger Geräte im Vergleich zur Gesamtzahl der verkauften Mobiltelefone nur sehr langsam zunehmen wird. Um NFC Anwendungen zum Durchbruch zu verhelfen, ist ein weitaus größerer Marktanteil NFC-fähiger Mobiltelefonen notwendig.



Abbildung 9: Größenvergleich – Transponderantenne in micro-SD Bauform

Aufgrund ihrer kleinen Abmessungen von $11 \text{ mm} \times 15 \text{ mm} \times 0,7 \text{ mm}$ (kaum größer als ein Fingernagel) werden in mobilen Endgeräten wie z.B. Mobiltelefonen als Speicherkarte für Fotos, Anwendungen und MP3-Files überwiegend micro-SD Karten verwendet. Es ist das weltweit kleinste Speicherkarten-Format und wird primär von Mobiltelefon-Herstellern wie Kyocera, Motorola, Samsung, Nokia und SAGEM sowie von GPS-Geräteherstellern wie Garmin und vereinzelt auch von MP3-Spieler-Herstellern unterstützt. Dies eröffnet die Möglichkeit, Mobiltelefone mit kontaktlosen micro-SD Karten nachzurüsten um so die Telefone mit einem kontaktlosen Interface auszustatten. Da für die micro-SD Karten vom Telefon eine Spannungsversorgung bereit gestellt wird, kann hier die beschriebene aktive Lastmodulation eingesetzt werden.

Gegenüber den herkömmlichen micro-SD Karten besteht eine kontaktlose micro-SD Karte mit aktivem RFID-Interface aus einigen zusätzlichen Komponenten. Neben dem üblichen Flash-Controller verfügt die kontaktlose micro-SD Karte grundsätzlich über ein sogenanntes Secure Element, üblicherweise ein Smart Card Chip mit eigenem Betriebssystem, z.B. STARCOS, SECCOS oder ein Java Card Betriebssystem. Das zur Anhebung der Lesereichweite benötigte aktive Lastmodulationssignal wird durch ein spezielles HF-Interface (Active RFID Interface) erzeugt. Das Secure Element übernimmt die Ansteuerung des aktiven RFID-Interfaces welches zum kontaktlosen Senden und Empfangen von Daten benötigt wird. Ein weiterer wichtiger Bestandteil ist die Antenne (vgl. **Abbildung 9**) welche aus einer einfachen Leiterschleife mit mehreren Windungen gebildet wird.

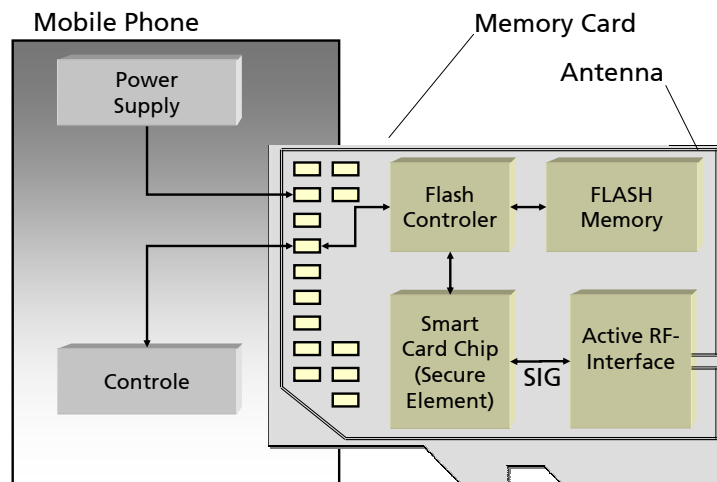


Abbildung 10: Die Komponenten der G&D micro-SD mit aktivem RFID-Interface.

Die Energie zum Betrieb der micro-SD Karte und des aktiven RFID-Interfaces wird durch das Mobiltelefon zur Verfügung gestellt und steht daher in ausreichendem Maße zur Verfügung. Ein besonderer Vorteil dieser Konstruktion besteht darin, dass ein entsprechendes Software Applet im Telefon über die micro SD Schnittstelle mit dem Secure Element kommunizieren kann. Auf diese Weise lässt sich das kontaktlose Interface bequem steuern und kontrollieren und der Status auf dem Display des Telefons angezeigt werden.



Abbildung 11: Zahlungsverkehrsterminal, Mobiltelefon und kontaktlose micro-SD Karte vor dem Einbau in das Telefon.

4 Der Weg in die Standardisierung

Ein Transponder mit aktiver Lastmodulation erzeugt ein Signal, welches für ein Lesegerät von einer klassischen Lastmodulation nicht zu unterscheiden ist. Trotzdem ergibt sich die

Notwendigkeit diese Technologie zu standardisieren. So schreibt die Norm ISO/IEC 14443-2 zum Beispiel zwingend die Verwendung eines passiven Lastmodulators vor, so dass ein Transponder mit aktiver Lastmodulation zum derzeit gültigen Standard schon aus diesem Grunde nie konform sein kann:

„Clause 8.2.2 – The PICC shall be capable of communication to the PCD via an inductive coupling area where the carrier frequency is loaded to generate a subcarrier with frequency f_s . The subcarrier shall be generated by switching a load in the PICC”.

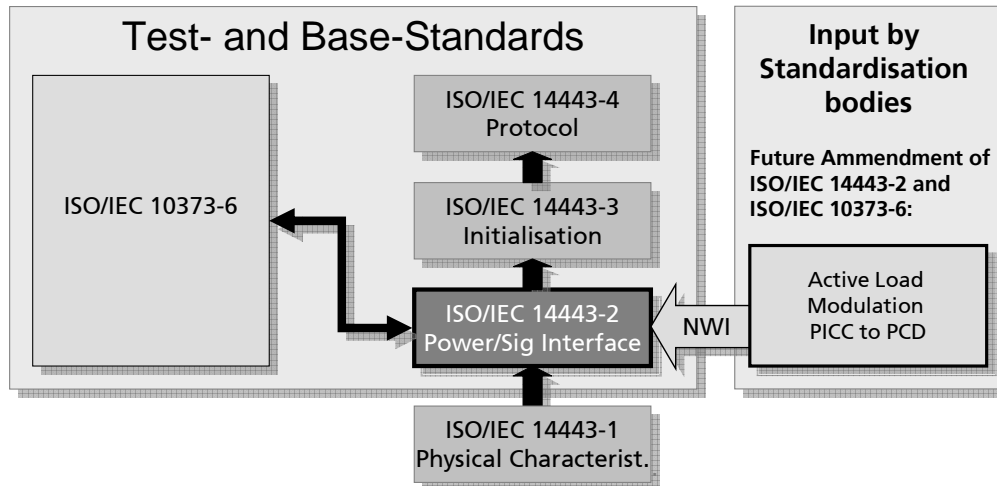


Abbildung 12: Die von aktiver Lastmodulation voraussichtlich betroffenen Test- und Basisstandards

Im Standard muss vor allem die Spezifikation der physikalischen Schnittstelle, also ISO/IEC 14443-2 sowie die dazugehörigen Compliance-Tests in ISO/IEC 10373-6 angepasst werden.. Neben der Neuformulierung einiger Abschnitte des Standards mit dem Ziel eine aktive Lastmodulation explizit zu erlauben, sind aber noch eine Reihe weiterer Fragen zu klären [WG8N1745].

“In order to be able to test these (active) PICCs independently from the numerous devices in which they can be inserted and also to test these devices independently from the PICCs which can be inserted in them, it was proposed to define a "Reference Active PICC". The same reasoning also applies for any other PICC which usually or always operates within a device.

The main objectives of the New Work Item Proposal were then clarified:

- Not to preclude the use of a battery (i.e. allow "active PICC modulation"), because present ISO/IEC 14443-2 explicitly defines "load modulation" for PICC;
- Define the RF limits for " Active PICCs" (independently from any device), so that these limits include margins to take typical device attenuation into account;
- Define the RF limits for devices, measured with a "Reference Active PICC.”

Um die Standardisierung dieses interessanten und zukunftsweisenden Themas anzustoßen, wurde im September 2010 ein entsprechender DIN Beitrag in SC17/WG8 eingereicht [WG8N1722] und auf der nachfolgenden Sitzung in Takamatsu (Japan) der WG8 vorgestellt. In der Folge wurde nun im Dezember 2010 durch SC17/WG8 ein NP Ballot mit folgendem Text gestartet [WG8N1755]:

„PICCs with external power supply – Use power supply other than the PCD-field so that PICCs with very small antenna and/or metallic environment can be compliant with ISO/IEC 14443-2:

Currently more and more small PICC form factors are penetrating the market. Very often these PICCs are attached on metal surfaces (mobile phones) or they are even operated inside a mobile phone (memory cards). These metal environments often cause additional drops in performance (reading distance).

WG8 has reacted with different antenna classes, which results in different ranges for the field strength for each class, thus resulting in reduced operating range for classes with increased minimum field strength.

Actively powering the PICC will allow the PICC to handle field strength down to 1,5 A/m even in metal environment, while transmitting an enhanced modulation signal will allow the PCD to pick up the PICC signal even with very bad mutual coupling between PICC and PCDs antenna, e. g. with metal environment. So PICCs with external power supply will be an innovative approach to operate very small PICC antennas with PCDs already in the field.”

5 Ausblick

Die Anwendung aktiver Lastmodulation ermöglicht es erstmals Transponder mit kleinsten Formfaktoren problemlos auch in einem System zu bereiten, welches ursprünglich für kontaktlose Chipkarten im ID1 Format entwickelt wurde. Erste Anwendungen in Bauform der micro- SD Karte für den Betrieb in einem Mobiltelefon zeigen das Potential hinter dieser neuen Technologie, gerade angesichts dessen, dass die Transponder mit der heute im Feld installierten Basis an Lesegeräten nach ISO/IEC 14443 voll kompatibel und interoperabel sind.

Literatur

- [BMI_10] Bundesministerium des Innern, Der neue Personalausweis, IT-Stab im Bundesministerium des Innern, <http://www.personalausweisportal.de/>
- [Fink08] Finkenzeller, Klaus, RFID Handbuch, 5. Auflage, Hanser Verlag München, 2008, S. 44-50, sowie http://rfid-handbook.de/downloads/G3E_3-446-22071-2_leseprobe.pdf
- [WG8N0165] SC17/WG8 N165, Terms of reference for SC17/WG8/TF2 „Remote coupling communication cards“ (RCCC), <http://wg8.de/WG8DocList.html>, 1993
- [WG8N1722] Finkenzeller, Klaus, Enhanced Modulation PICC to PCD, DIN Contribution, <http://wg8.de/WG8DocList.html>, -September 2010
- [WG8N1745] Roux, Pascal, Minutes of the 33rd meeting of WG8 Task Force 2, S. 7, <http://wg8.de/WG8DocList.html>, September 2010
- [WG8N1755] New Work Item Proposal, Revision 1, PICCs with external power supply, <http://wg8.de/WG8DocList.html>, Oktober 2010