NFC – was liegt näher?

Near Field Communication („Nahfeldkommunikation")

Der moderne Mensch kommuniziert heute auf vielfältige Art drahtlos, manchmal ohne sich dessen bewusst zu sein. Als Beispiel mag sein Handy, pardon Smartphone, dienen. Bereits bei seinem Einschalten bucht es sich automatisch in ein durch die eingesetzte SIM-Karte bestimmtes Funknetz ein. Dieser Vorgang läuft ohne Zutun des Nutzers ab. Nach Eingabe der PIN ist Telefonieren und Internetnutzung über das Netz des Anbieters möglich, mit dem der Nutzer vertraglich verbunden ist. Entsprechend eingestellt, nutzt das Smartphone für den Internetzugang automatisch ein WLAN-Netz oder „paart sich" mit Bluetooth-Geräten, wenn es in deren Wirkungsbereich gelangt.

Wozu ist nun eine weitere Technik der Kommunikation erforderlich? Ist man nicht mit Mobilfunk, WLAN und Bluetooth ausreichend versorgt? Bei genauerer Betrachtung stellt man fest, dass ein weiterer Ansatz namens Near Field Communication (NFC) sehr wohl seine Berechtigung hat und dem Anwender einen hohen Nutzen bietet.

Reichweite und Sicherheit. Eine Kommunikation soll nur unter berechtigten Teilnehmern möglich sein, meist zwei Personen oder technische Geräte. Es leuchtet unmittelbar ein, dass über größere Distanzen die grundsätzliche Möglichkeit des Mithörens oder Missbrauchs durch unbefugte Dritte mit konspirativen oder sabotierenden Absichten besteht. Je größer der Kommunikationsradius ist, umso vielfältiger sind die Möglichkeiten der unbefugten Fremdeinwirkung.

Ganz aktuell sind wir im doppelten Wortsinn „betroffen“ von den Aktivitäten der Geheimdienste, allen voran der amerikanischen National Security Agency (NSA). Sie nutzen vielfältige Möglichkeiten, die gigantischen Datenströme im World Wide Web anzuzapfen. Dies kann an Internetknoten, Übergabestationen für interkontinentale Überssee-Glasfaserkabel, durch Eingriffe in nationale Netze, Funknetzüberwachung, Einklinken in lokale Drahtlosnetze (WLAN) usw. geschehen. Das Ergebnis ist der „Gläserne Bürger“, dessen Rechte auf informationelle Selbstbestimmung aus vorgeblichen Gründen der Terrorabwehr entgegen Recht und Gesetz missachtet werden. Ganz zu schweigen von Cyberkriminellen, die mit illegal erlangten Daten ihre Betrugsabsichten in die Tat umsetzen können.

NFC (Near Field Communication = Nahfeldkommunikation) mit einem Aktionsradius von wenigen Zentimetern bietet aus sich heraus bereits ein extrem hohes Maß an Sicherheit. Wegen der kurzen Reichweite ist nur die Kommunikation zwischen zwei Teilnehmern möglich, der „Dritte Mann“ oder ein „Man in the Middle“ findet keine Möglichkeit, den Prozess des Informationsaustauschs zu erkennen, in ihn einzudringen oder die Teilnehmer zu lokalisieren. In der direkten Kommunikation zwischen zwei Menschen ist das vergleichbar mit dem Gespräch im Flüsterton, mit dem Mund am Ohr des Gesprächspartners.

NFC kann als reichweitenschwache Variante „Close Coupling“ (enge Kopplung) von RFID (Radio Frequency Identification) angesehen werden (Bild 1). Je nach Kopplungsdistanz zwischen den Kommunikationsteilnehmern unterscheidet man Long-Range Coupling (Weitbereichskopplung), Vicinity Coupling (Nachbarschaftskopplung), Proximity Coupling (Nahbereichskopplung) und Close Coupling (enge Kopplung). Bei der für NFC eingesetzten engen Kopp-

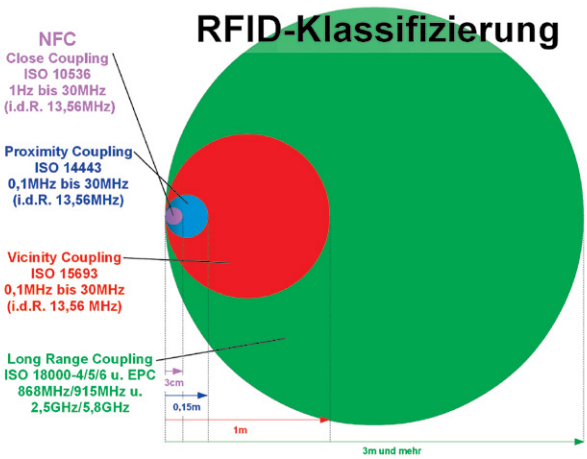

Bild 1: Radio Frequency Identification (RFID) kennt verschiedene Reichweiten. NFC deckt den Bereich von wenigen Zentimetern ab (Close Coupling).

lung wird das Nahfeld einer Sendespule ausgewertet. Es wird durch die Terme in den Maxwell'schen Feldgleichungen dominiert, die mit wachsender Entfernung zur Antenne schnell abnehmen und deshalb bei größeren Entfernungen, also im Fernfeld, vernachlässigbar sind [http://de.wikipedia.org/wiki/Nahfeld_und_Fernfeld_(elektromagnetische_Wellen)]. Durch ihre geringe Reichweite sind bei NFC-Kommunikationen Überlagerungen praktisch ausgeschlossen. Deshalb braucht kein Aufwand für die Vermeidung von Kollisionen betrieben zu werden. Die praktische Unmöglichkeit der Manipulation macht zudem eine Verschlüsselung der Daten in der Regel überflüssig. Das macht NFC-Tags besonders energieeffizient.

NFC-Ursprung und Eigenschaften. Im Jahr 2002 initiierten Philips (Tochterunternehmen NXP) und Sony NFC als drahtlose Übertragungstechnik zwischen Geräten mit einem Abstand von typisch 1 bis 4 cm. Heute sind im 2004 gegründeten NFC-Forum (www.nfc-forum.org) mehr als 170 Mitglieder vereint, um die Interoperabilität zwischen Geräten und Diensten sicherzustellen. Hersteller, Anwendungsentwickler, Finanzdienstleister und Weitere arbeiten zusammen, um die NFC-Technologie in der Unterhaltungselektronik, bei mobilen Geräten und PCs zu fördern.

NFC-Technologie arbeitet im Nahfeld einer elektromagnetischen Strahlung durch induktive Kopplung in einem lizenzfreien Frequenzbereich von 13,56 MHz und ermöglicht die kontaktlose Datenübertragung über wenige Zentimeter (typisch 1–4 cm, maximal 10 cm) mit Datenraten von 106 Kbit/s, 212 Kbit/s und 424 Kbit/s. Das hat den Vorteil kleiner, billiger und wenig Energie verbrauchender Sender und Empfänger, die reichweitenbedingt keine Rücksicht auf andere NFC-Kommunikationen in der Umgebung nehmen müssen. Wir haben es hier mit einem klassischen drahtlosen, frequenzökonomischen Raummultiplexverfahren zu tun, denn außerhalb des Wirkungsbereichs mit den Ausmaßen einer Raumzelle von wenigen Zentimeter Durchmesser kann die gleiche Frequenz wiederbenutzt werden.

Die Kommunikation findet stets nur zwischen zwei Teilnehmern statt – Initiator (Auslöser, im Englischen auch Polling Device oder Poller – Interviewer – genannt) und Target (Ziel, im Englischen auch Listening Device oder Listener – Hörer – genannt). Wie es der Name sagt, stößt der Initiator eine Transaktion an, indem er dem Target eine Information sendet und es zu einer Reaktion auffordert.

Man unterscheidet zwei NFC-Kommunikationsmodi, den passiven Modus (passive mode) und den aktiven Modus (active mode).

- Im **aktiven Modus** benötigen sowohl Initiator als auch Target eine eigene Energiezufuhr und erzeugen für die Datenübertragung jeweils ihr eigenes RF-Magnetfeld (RF: Radio Frequency = Hochfrequenz).
- Im **passiven Modus** erzeugt nur der Initiator ein RF-Magnetfeld. Das passive Target moduliert dieses, um Daten zu übertragen. Die dafür erforderliche Energie kann es aus dem Feld beziehen, benötigt somit keine eigene Energiezufuhr.

Die Elektronik eines passiven Targets kann also durch das Bestrahlen mit einem RF-Magnetfeld aus dem Schlaf geweckt werden und dann nach einem Handshake-Prozess zur Konfiguration der Teilnehmer mit der Datenübermittlung beginnen. Dafür ist kein selbsterzeugtes RF-Magnetfeld erforderlich. Es genügt, dem vom Initiator erzeugten Magnetfeld auf spezifische Weise Energie zu entziehen, was der Initiator als Information interpretiert. Man spricht bei dieser informationsgesteuerten Rückwirkung auf die Amplitude des Initiatorfeldes von einer Lastmodulation. Bei den Betriebsmodi kann man drei Fälle unterscheiden:

- **Read/Write.** In diesem Modus (Deutsch: Lesen/Schreiben) kann der Initiator (z. B. ein NFC-fähiges Handy) von jedem NFC-Target (meist ein NFC-Tag) Daten auslesen oder in es einschreiben.
- **Peer to Peer.** In diesem Modus können zwei NFC-Geräte gleichberechtigt Daten austauschen. So lassen sich z. B. die Parameter zum Aufbau einer Bluetooth- oder WLAN-Verbindung wechselweise mitteilen. Der Peer-to-Peer-Modus ist in ISO 18092 spezifiziert.
- **Card Emulation.** In diesem Modus kann ein NFC-Lesegerät die Rolle eines NFC-Tags für andere Lesegeräte übernehmen. Damit wird die Rolle von Initiator und Target vertauscht.

Das Datenaustauschformat wird als NDEF (NFC Data Exchange Format) bezeichnet. Auf der Homepage des NFC-Forums und bei Nokia (http://developer.nokia.com/info/sw.nokia.com/id/bdaa4a0f-fcf3-4a4b-b800-c664387d6894/Introduction_to_NFC.html) finden sich detaillierte Beschreibungen. Grob kann man sagen, dass eine NDEF-Message aus mehreren Records besteht, die jeweils einen Header (Nachrichtenkopf) und eine Payload (Nutzdaten) enthalten. Der Header wiederum setzt sich aus Identifier sowie Angaben zu Länge und Typ der Payload zusammen (Bild 2).

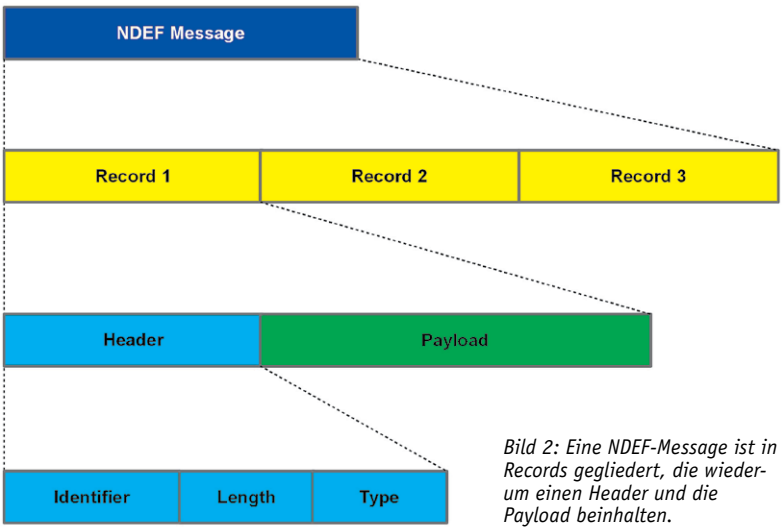

Bild 2: Eine NDEF-Message ist in Records gegliedert, die wiederum einen Header und die Payload beinhalten.

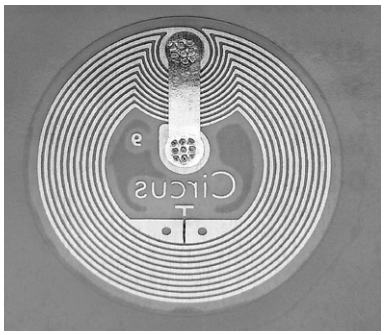

Bild 3: Typischer passiver NFC-Tag in Form eines Stickers (Hama-NFC-Sticker for Smartphone, 00015684) mit einer Kantenlänge von 35 mm

Aufbau und Funktionsweise eines NFC-Tags. Bild 3 zeigt ein typisches passives NFC-Modul (auch NFC-Tag genannt) der Firma HAMA (NFC-Sticker for Smartphone, 00015684). Deutlich erkennt man die Spule, über die induktiv Betriebsenergie aus dem RF-Magnetfeld des Initiators für den Chip in der Mitte gewonnen wird und die Lastmodulation des Feldes stattfindet. Schaut man sich diesen Tag genauer mit einem Leseprogramm an, z. B. NFC Tools, findet man als

Hersteller NXP und einiges mehr heraus (Bild 4). Am Ersatzschaltbild der für die an der Lastmodulation beteiligten Komponenten in Bild 5 lässt sich die Funktionsweise erläutern. Der Initiator (z. B. ein NFC-fähiges Mobiltelefon als Lesegerät) erzeugt über die Initiatorspule L1 ein hochfrequentes Wechselfeld. In der Spule L2 im Target (z. B. eine Chipkarte) wird dadurch eine Spannung induziert, die zur Speisung des NFC-Chips dient. Dieser moduliert nun die Lastimpedanz, was sich wiederum über den von L1 und L2 gebildeten Transformator auf den Initiator überträgt. Die den zu übertragenden Daten entsprechenden Schwankungen der Lastimpedanz werden im Initiator ausgewertet, wodurch auch hier die im Target abgelegte Datenfolge zur Verfügung steht. Damit ist eine Datenübertragung von der Chipkarte zum Handy vollzogen, ohne dass der NFC-Chip in der Chipkarte ein eigenes Feld erzeugen musste.

Den Kommunikationsvorgang zwischen auslösendem Gerät (Initiator, Reader) und dem NFC-Tag als reagierendem Gerät (Target, Listener) fasst Bild 6 zusammen. Im Nahbereich des vom NFC-Reader erzeugten elektromagnetischen Feldes wird durch Induktion in der Spule des NFC-Tags eine Spannung induziert, die den Tag-Chip mit Betriebsenergie versorgt und veranlasst, seinen gespeicherten Daten entsprechend auf die Amplitude des Feldes zurückzuwirken, d. h. es zu modulieren. Aus den Feldschwankungen gewinnt der NFC-Reader die modulierenden Daten wieder.

Bei NFC wird eine Spiralspule als Sende- bzw. Empfangsantenne eingesetzt. Diese produziert im Nahbereich je ein quasistatisches magnetisches und elektrisches Feld (H- und E-Nahfeld, Intensitätsabnahme mit $1/r^3$). Die Ausbreitung in den Raum beginnt erst in ausreichend großem Abstand durch kohärente Kombination von E- und H-Feld zur ebenen elektromagnetischen Welle (Fernfeld, Intensitätsabnahme mit 1/r). Nur im Nahfeld ist die magnetische Feldstärke groß genug, um zwischen zwei Spulen nennenswerte Energien durch magnetische Induktion auszutauschen. In der Praxis zeigt sich, dass diese nur bis zu einem Antennenabstand in der Größenordnung des Spulendurchmessers gut nutzbar ist. Bild 7 zeigt die magnetische Feldstärke H einer Spule im Abstand von 20 mm in Abhängigkeit vom Spulendurchmesser. Man sieht, dass bei einem Durchmesser von 20 mm die Feldstärke am größten ist. Weil das Magnetfeld mit wachsender Distanz sehr stark (60 dB/Dekade) abklingt, kann es dort nicht mehr zur Energieversorgung eines passiven NFC-Tags oder zur Datenübertragung per Lastmodulation dienen. Im Grunde haben wir es mit einem Transformator mit schwach gekoppelten Wicklungen zu tun.

Im nächsten Teil des Artikels beschreiben wir die verschiedenen Tag-Typen, die Sicherheitsaspekte sowie die zahlreichen Anwendungsbeispiele.

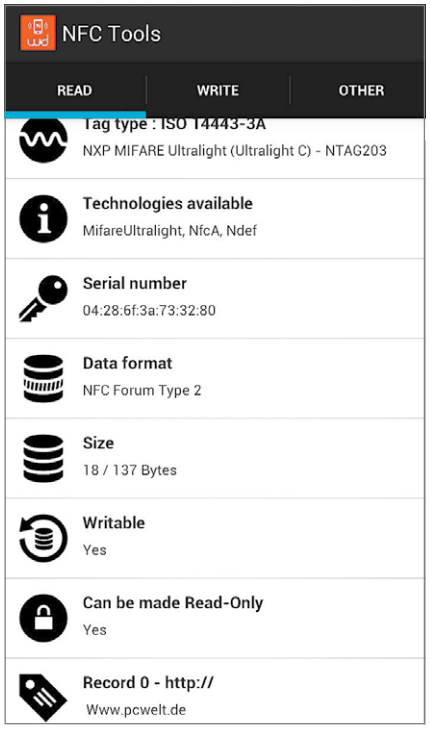

Bild 4: Mit Hilfe eines Lesegeräts gibt der NFC-Tag aus Abbildung 3 eine Vielfalt von Informationen über sein Innenleben preis.

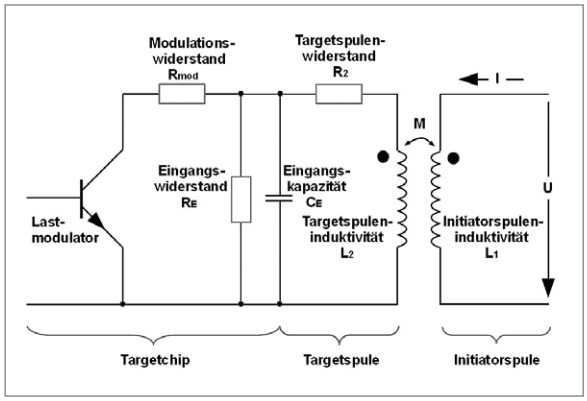

Bild 5: Die Spulen in Initiator und Target bilden einen lose gekoppelten Transformator, der Betriebsenergie für den NFC-Chip im Target überträgt und die von diesem initiierten Lastschwankungen auf die Initiatorseite zur Auswertung zurückmeldet.

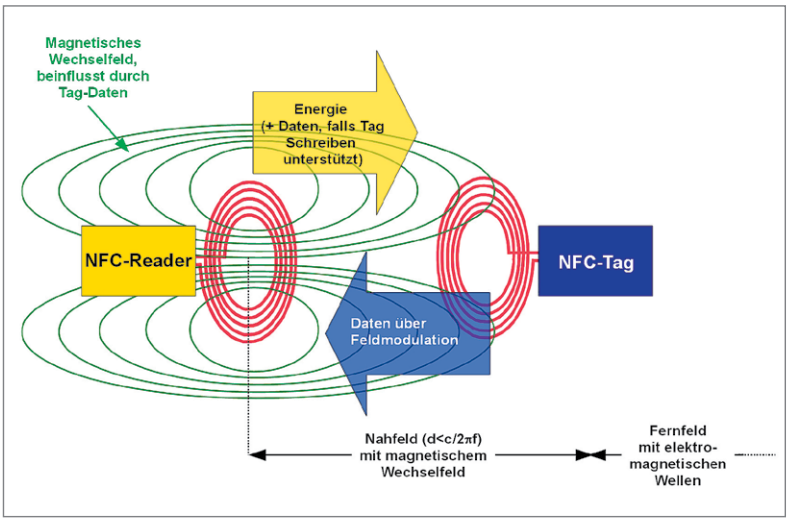

Bild 6: Der Reader baut ein Magnetfeld auf, das den NFC-Tag aktiviert, der daraufhin durch Lastmodulation des Feldes seine Daten preisgibt.

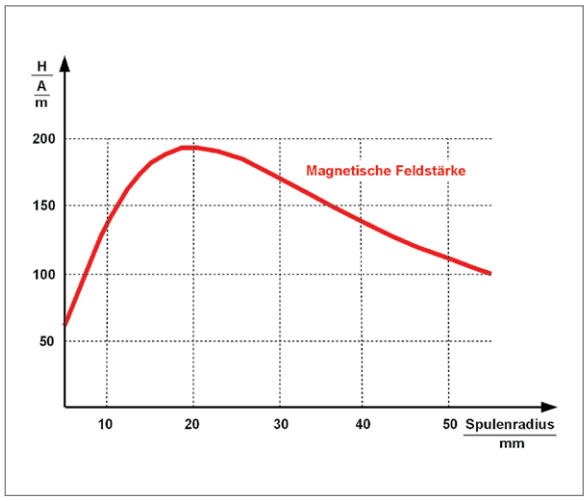

Bild 7: In einem Abstand von 20 mm erzeugt eine Spule mit 20 mm Radius die maximale magnetische Feldstärke.
Quelle: Tenec/Semiconductor