



NFC – was liegt näher?

Teil 2: 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.



Im ersten Teil des Artikel berichteten wir über die Reichweite und Sicherheit, den Ursprung und den Aufbau des NFC-Tags – weiter geht's mit Teil 2 des Artikels!

NFC-Tag-Typen. Es wurden vier Basistypen von Tags definiert. Sie unterscheiden sich in Format und Kapazität und beruhen auf den ISO-14443-Typen A und B (Standard für kontaktlose Smartcards) und ISO 18092 (Sony FeliCa, Standard für die passive Kommunikationsart). Die wichtigsten Kenngrößen der vier Typen fasst [Bild 8](#) zusammen.

NFC-Kommunikationsabläufe werden durch Protokolle geregelt. Diese sind in einschlägigen Normen beschrieben, um die Kompatibilität von NFC-Komponenten unterschiedlicher Hersteller zu gewährleisten. Detailinformationen sind unter www.nfc-forum.org/specs/spec_list zu finden.

Wegen der Nahfeldeigenschaft von NFC ist nur ein Short-Range-Protokoll erforderlich. Dabei muss nicht wie bei anderen Long-Range-Protokollen (z. B. für Bluetooth oder WLAN) zwingend darauf geachtet werden, dass aus der Vielzahl der potentiellen Kommunikationspartner innerhalb des Reichweitereichs die richtigen zueinander finden, um sich gegenseitig zu parametrisieren und die Übertragung durchzuführen. Bei NFC genügt es, die Geräte aneinander zu halten, und die Verbindung wird automatisch hergestellt. Weil hier eine offensichtlich gewollte Kommunikation zwischen zwei ausschließlich möglichen Partnern stattfinden soll, ist eine gegenseitige, verifizierte Identifikation nicht erforderlich.

Quelle: NFC-Forum	Tag-1-Typ	Tag-2-Typ	Tag-3-Typ	Tag-4-Typ
Kompatible Produkte	Broadcom Topaz	NXP Mifare Ultralight NXP Mifare Ultralight C NXP NTAG203	Sony FeliCa	NXP DESFire NXP SmartMX-JCOP
Speichervolumen	98 Byte	48/144 Byte	1/4/9 kByte	4/32 kByte
Stückpreis	niedrig	niedrig	hoch	mittel/hoch
Datenzugriff	Lesen/Schreiben oder Nur-Lesen	Lesen/Schreiben oder Nur-Lesen	Lesen/Schreiben oder Nur-Lesen	Lesen/Schreiben oder Nur-Lesen
Übertragungsgeschwindigkeit	106 kbit/s	106 kbit/s	212 kbit/s	106 ... 424 kbit/s
Norm	ISO14443A	ISO14443A	Sony FeliCa ISO18092	ISO14443A/B

Bild 8: Die Tabelle gibt eine grobe Übersicht über die Tag-Typen und ihre wichtigsten Eigenschaften.

Sicherheitsaspekte. Trotz der geringen Reichweite und der Tatsache, dass eigentlich nur zwei Kommunikationspartner eine Verbindung aufbauen können, ist auch bei NFC ein Restrisiko des Missbrauchs gegeben. Zum Beispiel könnte ein Cyberkrimineller in der überfüllten U-Bahn, wo sich körperliche Berührungen nicht vermeiden lassen, über NFC die Übertragung sensibler Daten oder das Ausführen von schädlichen Befehlen trotz der geringen Reichweite bewirken. Dieses Szenario ist zwar extrem unwahrscheinlich, aber auch nicht unmöglich. Wer auf Nummer Sicher gehen will, kann sich eine Hülle mit Schirmwirkung für seine Karten mit NFC-Chip kaufen (www.cryptalloy.de). Einen weiteren Sicherheitsgewinn bringt die Verschlüsselung der auf dem NFC-Tag abgelegten Daten.

Bezahlvorgänge mit dem NFC-fähigen Handy und einer entsprechenden App sind dank des eingesetzten CVC3-Verfahrens (CVC: Card Validation Code) sicherer als mit einer klassischen Kreditkarte. Das liegt daran, dass im Gegensatz zu den statischen CVC1-Codes der Kreditkarten der CVC3-Code dynamisch ist. Ein heimtückischer Spion könnte zwar theoretisch einige Informationen aus dem Smartphone auslesen, daraus jedoch nicht genügend viele weitere für eine nachfolgende Transaktion extrahieren. Dafür ist ein CVC3-Berechnungsschlüssel erforderlich, der zur Erzeugung des für eine Transaktion erforderlichen einzigartigen CVC3-Codes im sogenannten „Sicheren Element“ des Mobiltelefons gespeichert ist. Als „Sicheres Element“ wirken in einem Mobiltelefon ein SIM (Subscriber Identity Module), eine Speicherkarte und ein eingebauter Chip zusammen. Ein einmal ausspionierter Code ist bei der nächsten Transaktion ungültig und deshalb wertlos. Hinzu kommt eine 112-Bit-Verschlüsselung, so dass man den CVC3-Algorithmus als die derzeit sicherste Authentifizierungsmethode betrachten kann.

Zweifellos liegt im Verlieren des Handys das größte Risiko. Deshalb kann man viele Smartphones heute mit einer geeigneten Security-Software über die Mobilfunkverbindung orten und sperren. Als ultimative Maßnahme kommt das Löschen der sicherheitskritischen Daten auf dem verlorenen Handy aus der Ferne in Frage.

Anwendungsbeispiele. Die meisten NFC-Anwendungen basieren heute auf Smartphones mit NFC-Funktion. Im Folgenden werden einige aus der nur durch die Fantasie beschränkten Vielfalt beschrieben.

Elektronisches Bezahlen



Hier ist M-Commerce (Mobile Commerce: mobiler Handel), das Bezahlen unter Verwendung drahtloser Kommunikation und des Mobiltelefons (electronic payment) weltweit sicher die häufigste NFC-Anwen-

dung. Dabei unterscheidet man zwischen Micropayment für Summen zwischen 0 und 5 Euro und Makropayment für darüber liegende Beträge.

Mittlerweile gibt es eine große Vielfalt elektronischer Bezahlssysteme: billpay, bitcoin, clickandbuy (Firstgate), EBPP (Electronic Bill Presentation and Payment), girogo, iclear, micropayment, net900, PayBox, Paymill, Paymorrow, Paynova, PayPal, PayPass, Paysafecard, Scril (ehem. Moneybookers), SET (Secure Electronic Transaction), Wirecard ...

Aus Nutzersicht sind von allen E-Payment-Systemen einige Anforderungen zu erfüllen: Anonymität (Kaufvorgänge und Kaufgewohnheiten sollen nicht nachvollziehbar sein), Unverkettbarkeit (Zahlungen sollen durch Bank oder Händler wegen der Forderung nach Anonymität und Unbeobachtbarkeit nicht zuordenbar sein), Sicherheit (Datenintegrität, Authentifizierung, Autorisierung, Nichtabstreitbarkeit). Händler haben freilich oft ganz andere Interessen. Sie wollen aus der Abfolge elektronischer Bestell- und Bezahlvorgänge eines Kunden ein auf ihn zugeschnittenes Werbeprofil generieren. An dieser Stelle ist der Datenschutz zur Wahrung der informationellen Selbstbestimmung besonders gefordert. Sonst könnte es durchaus möglich sein, dass das Bezahlen von Zigaretten am NFC-fähigen Automaten zu Einträgen in die Mitgliederakte der Krankenkasse führt oder „Vater Staat“ Bewegungsprofile seiner Bürger erstellt. Die Vision von „Big Brother is Watching You“ darf nicht noch konkretere Formen annehmen.

Touch&Travel



Bild 9: Wo auf Bahnhöfen das Touch&Travel-Logo zu sehen ist, kann man ohne Fahrkartenschalter quasi im Vorbeigehen sein virtuelles Reiseticket auf das NFC-fähige Handy laden.

Touch&Travel ist eine ticketlose Art der Buchung einer Reise mit den Verkehrsmitteln der Deutschen Bahn (DB) – Zug oder Bus. Zur Nutzung benötigt man ein NFC-fähiges Funktelefon (Handy) und sogenannte Kontaktpunkte, gekennzeichnet durch das Logo in [Bild 9](#), am Start- und Zielbahnhof. Vor der Nutzung von Touch&Travel muss man sich registrieren und die Touch&Travel-App auf das Handy laden.

Der Erwerb einer Reiseberechtigung sieht nun so aus:

- **Beginn der Reise mit Touch-in:** Handy mit Touch&Travel-App an Touchpoint im Startbahnhof halten, damit Handy die Positionsdaten des Touchpoints auslesen kann. Handy übermittelt diese via Mobilfunk an den Ticketserver der DB, der eine Fahrtberechtigung an das Handy zurückgibt. Nun kann der Fahrgast einsteigen.
- **Kontrolle während der Reise:** Zur Überprüfung der Fahrtberechtigung wird dem Kontrollpersonal einfach das Handy gezeigt. Dieses zeigt auf der Kontrollseite der App einen Barcode, den der Kontrolleur mit Hilfe eines Kontrollgerätes liest.
- **Beenden der Reise mit Touch-out:** Am Ende der Fahrt Handy an einen Touchpoint des Zielbahnhofs halten. Nach einer Kommunikation mit dem Ticketserver übermittelt dieser dem Handy den Fahrpreis und löscht die Fahrtberechtigung.
- **Bezahlen der Reise:** Ticketserver übergibt Reisedaten an Rechnungsserver. Der erstellt Rechnung, die dem Reisenden per E-Mail zugestellt wird. Die Bezahlung der Rechnung erfolgt per Lastschrift. All das ist mit keinerlei Eingaben oder sonstigen Interaktionen mit dem Handy verbunden, also äußerst schnell, bequem und sicher. Verfügt das Handy über keine NFC-Funktion, kann man auch jeweils am Start- und Zielbahnhof die Positionsbestimmung nutzen oder den auf dem Kon-



taktpunkt aufgedruckten Barcode scannen oder die aufgedruckte Nummer des Kontaktpunktes eingeben. Das hat natürlich nicht den Charme der NFC-Lösung.

Tourismus



In einer Beschreibung der Mess- und Prüftechnik für NFC-Technologie

(www.rohde-schwarz.de/file/NEWS_208_german_SMx-K89.pdf) von Rohde&Schwarz wird von einer NFC-Anwendung auf den Berggipfeln des polnischen Nationalparks Hohe Tatra berichtet (Bild 10). Wanderer können mit Hilfe eines NFC-fähigen Smartphones und einer entsprechenden App ihren elektronischen Wanderpass mühelos ausfüllen. Dazu brauchen sie nur auf jedem erreichten Gipfel ihr Gerät an die hier angebrachten NFC-Tags zu halten.

Diese Methode ist natürlich auf vielfältigste Art und Weise im Tourismus anwendbar. Als elektronischer Stadtführer, in Museen, Kunstgalerien, Burgen usw.

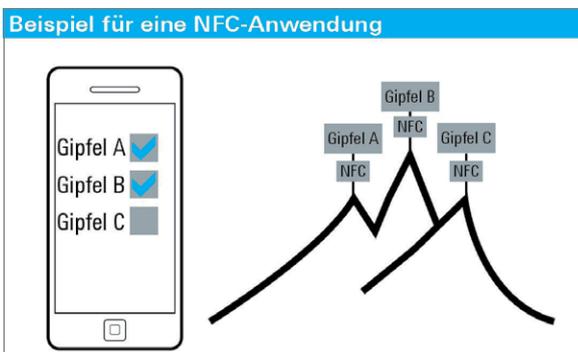


Bild 10: Der elektronische Wanderpass auf einem Handy wird vom NFC-Tag auf den Gipfeln der Hohen Tatra ausgefüllt. Quelle: Rohde&Schwarz

Als eines von mittlerweile vielen weiteren Beispielen sei der Online-Stadtführer der hessischen Stadt Lich genannt (www.geschichtlich.info). Hier sind an besonderen Sehenswürdigkeiten mit QR-Codes kombinierte NFC-Chips angebracht. Besitzer von Smartphones mit Kamera oder NFC-Reader können diese durch Fotografieren oder Annähern scannen, um direkt zur Beschreibung des Gebäudes zu gelangen (Bild 11). Voraussetzung ist ein mobiler Internetzugang für das Smartphone. Angesichts der hohen Speicherkapazitäten moderner Smartphones wäre es natürlich auch möglich, den elektronischen Stadtführer auf das Smartphone zu laden und die Informationen offline durch die NFC-Tags auszuwählen.

Identifikation



Eine naheliegende Anwendung im Umfeld des Automobils ist der Einsatz des NFC-Smart-



Bild 11: Der Online-Stadtführer der hessischen Stadt Lich

phones als Autoschlüssel zum Türöffnen und Starten. Beispielsweise kann der Autofahrer sein Smartphone in die Nähe eines NFC-Tags auf der Scheibe bringen, um sich zu identifizieren und das Fahrzeug zu öffnen oder zu schließen. Hat der Fahrer hinter dem Lenkrad Platz genommen, kann die Fahrzeugelektronik z. B. über Bluetooth Kontakt mit dem Smartphone aufnehmen und sein personalisiertes Nutzerprofil laden und umsetzen. Das könnte die Entriegelung der elektronischen Wegfahrsperrung, automatische Sitz- und Spiegeleinstellung, Wahl der Lieblingsradiostation, Einstellung der bevorzugten Temperatur, Einbinden des Smartphones in das Soundsystem als Freisprecheinrichtung und in das On-Board-Diagnosesystem (OBD) usw. sein. Angesichts des sich abzeichnenden Trends zum Car-Sharing sind dies äußerst sinnvolle, den Komfort der Nutzer steigernde Funktionen.

Ein weiteres Beispiel kommt aus Japan. Hier werden bereits vielfach die Identifikationsdaten von Studenten auf deren NFC-fähige Smartphones geladen. Ein Student kann sich damit elektronisch für Vorlesungen einschreiben, in der Mensa bezahlen, in der Bibliothek Bücher ausleihen, Türen zu Bereichen öffnen, für deren Zutritt er berechtigt ist, Ermäßigungen in Kinos, Restaurants und Läden erhalten und sich mit Kommilitonen Informationen durch einfaches Aneinanderhalten der Smartphones teilen.

Lesen, Editieren und Beschreiben von NFC-Tags

Zum Lesen eines NFC-Tags wird hier als Lesegerät ein NFC-fähiges Smartphone Samsung GT-I9300 (Galaxy S3) mit Android-Betriebssystem Version 4.1.1 eingesetzt (Bild 12). Im Internet findet sich eine Vielzahl von teilweise kostenlosen Android-Programmen für Mobilgeräte (Apps) zum Lesen, Löschen, Editieren und Beschreiben eines NFC-Tags.

Jedes der Programme hat seine Stärken und Schwächen. Wenn man nur wissen will, von welchem Typ ein Tag ist und welchen Inhalt er hat, ist die Tag-Analyse-Funktion des inViu-NFC-Trackers sehr auskunftsfreudig (Bild 13).

Eine einfach anzuwendende App ist der NXP Tag-Writer. Wird er auf dem Handy geöffnet und dieses an



Bild 12: Das Samsung Galaxy S3 ist eines von mittlerweile vielen Smartphones, die für die Nutzung von NFC-Anwendungen geeignet sind.

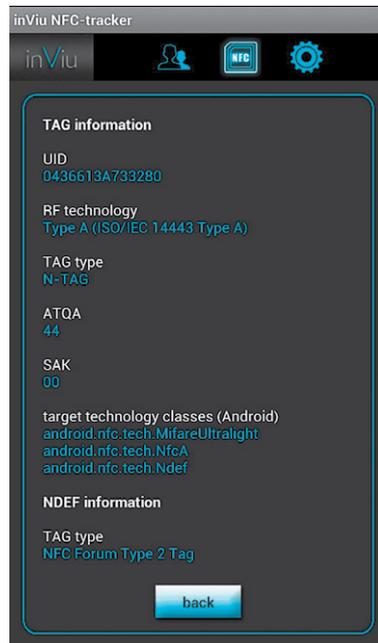


Bild 13: Der inViu-NFC-Tracker gibt Auskunft über das Innenleben eines NFC-Tags.

einen NFC-Tag gehalten, liest der TagWriter einen darauf gespeicherten Steuerbefehl für das Handy, zeigt ihn an und führt ihn auf einen Klick aus. Ebenso kann er den Steuerbefehl selbst erzeugen und auf den Tag schreiben.

Ein Beispiel: Wir möchten einen Tag überschreiben (er enthält bereits die Kontaktdaten von Albert Huang), der bei Annäherung des Smartphones die Homepage www.web.de aufruft. Dazu gehen wir auf den Menüpunkt „Create and write“ und definieren einen neuen NFC-Datensatz. Jetzt wählen wir „URL“ und legen eine neue „Bookmark“ an. Hier

tragen wir „web.de“ ein, drücken „Next“ und setzen das Häkchen zur Bestätigung des Überschreibens eines eventuell bereits vorhandenen Tag-Inhalts. Noch einmal „Next“ drücken, und wir werden aufgefordert, den NFC-Tag mit dem Handy zu berühren, um ihn zu beschreiben. Ist das geschehen, genügt es in Zukunft, mit dem eingeschalteten Handy diesen Tag zu berühren, und es öffnet sich automatisch der Webbrowser, um sich ohne weiteres Zutun auf www.web.de einzuloggen. Die beschriebene Abfolge der Schritte fasst Bild 14 zusammen.

NFC als Leinenwerfer. Hierbei dient NFC nur zum One-Touch-Aufbau einer Verbindung über eine reichweiten- und bandbreitenstärkere Technologie wie Bluetooth oder Wi-Fi.

Ein Beispiel ist der Thomson NFC-Musikempfänger „AR 6103“ (ELV-Best.-Nr.: JQ-11 15 82). Er dient der kabellosen Musikübertragung via Bluetooth 3.0 von mobilen Endgeräten zur Hi-Fi-Anlage mit einer maximalen Reichweite von ca. 10 m. Die Bluetooth-Verbindung lässt sich dabei durch NFC-Technologie schnell und bequem aktivieren: Handy an den im „AR 6103“ integrierten NFC-Chip oder den mitgelieferten externen annähern, und schon liest das Handy die Einstelldaten für die Bluetooth-Verbindung ein, paart sich mit dem „AR 6103“, und die Übertragung von digitalen Audiodateien als MP3-Streams kann beginnen. Der „AR 6103“ gibt die via Bluetooth-Funktechnik empfangenen Streams in Echtzeit entweder drahtgebunden als analoge Links- und Rechtssignale an die Cinch-Eingänge oder digital via POF (polymere optische Faser) an den optischen S/PDIF-Eingang (Sony/Philips Digital Interface oder

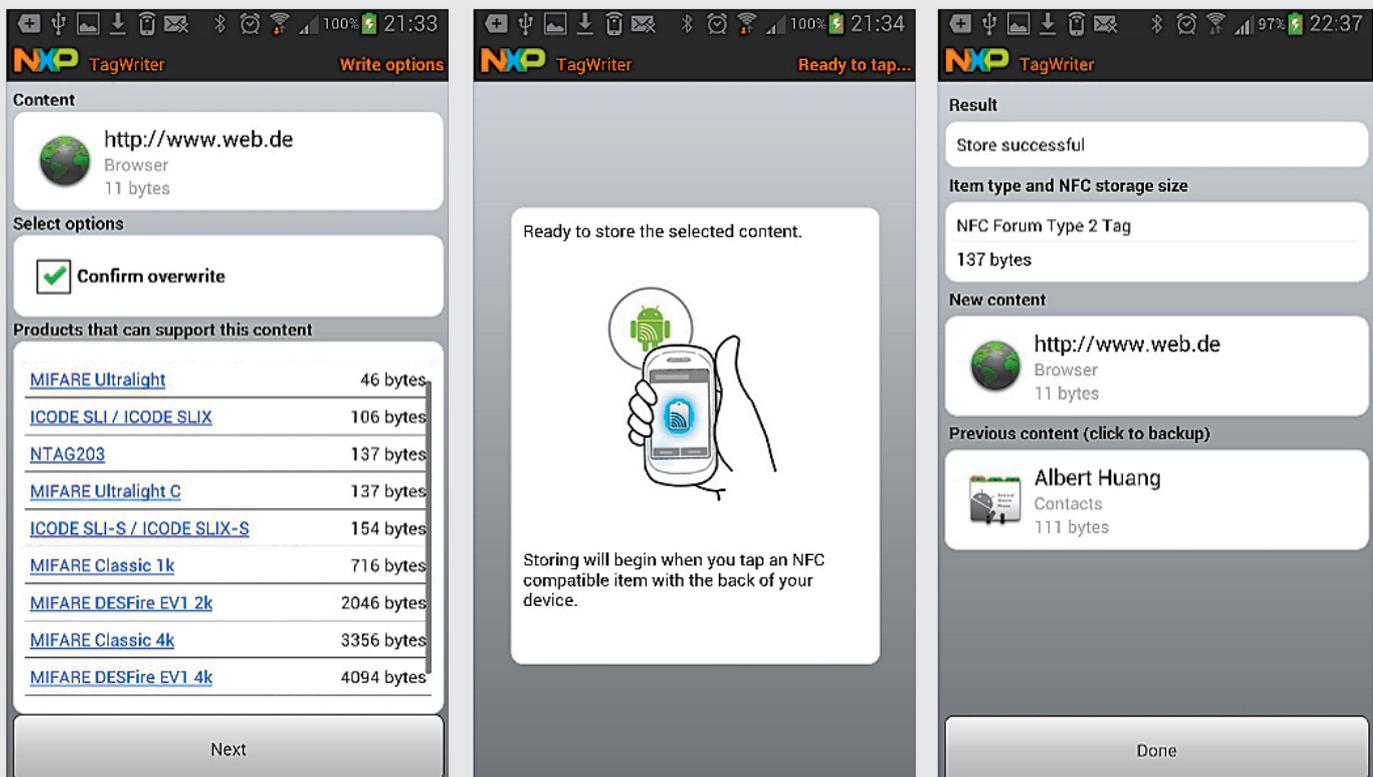


Bild 14: Der Vorgang des Tag-Beschreibens in Einzelschritten demonstriert.

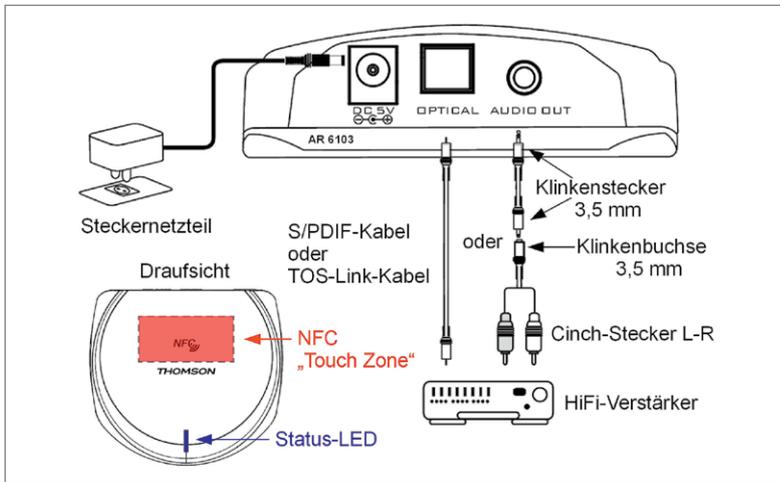


Bild 15: Der Music-Streamer „AR 6103“ von Thomson empfängt per Bluetooth Audiosignale vom Smartphone und gibt sie als optische oder elektrische Signale leitungsgebunden an die Hi-Fi-Anlage weiter. Die Konfiguration des Handys beschränkt sich auf die Berührung eines NFC-Tags.

TOS-Link) des Hi-Fi-Verstärkers weiter (Bild 15). Sollte das verwendete Handy über keine NFC-Funktionalität verfügen, kann man es natürlich auch „klassisch“ per Hand mit dem „AR 6103“ verbinden. Die Einfachheit einer „One-Touch“-Konfiguration geht dabei natürlich verloren.

Mit dem „AR 6103“ konnte die Uralt-Stereoanlage des Autors (Bild 16) aus den frühen 1980er-Jahren (Sansui, A-80-Verstärker, T-80-Tuner) mühelos den Anschluss an die Moderne finden. Es ist eine schöne Sache, bequem auf dem Sofa liegend (wenn das ein favorisierter Aufenthaltsort ist, sollte man auch hier den NFC-Tag anbringen) vom Handy seine Lieblingsongs abzuspielen, Klang und Lautstärke zu wählen oder die Musikwiedergabe bei einem Telefonanruf stumm zu schalten.

Mit einer 64-GB-Byte-microSD-Karte im Handy ist die Anzahl der Songs ja bereits riesig. Noch mehr ist aber jederzeit möglich, wenn man mit

dem Handy die Stücke auf dem Home-Medienserver mit seiner Speicherkapazität im Terabyte-Bereich via lokalem WLAN abgreift und per Bluetooth an den „AR 6103“ weiterleitet. Und mit Internetradio ist die Vielfalt praktisch grenzenlos.

Fazit

NFC bietet eine nahezu unbegrenzte Fülle äußerst sinnvoller Anwendungen in den Bereichen „Payment & Ticketing“, „Electronic Keys“, „Identification“, „Reception & Sharing of Information“, „Set-up Services“ usw. Damit ist NFC die ideale ergänzende Nahbereichstechnologie für das „smarte“ Mobiltelefon mit seinen weiter reichenden Funktechniken GSM, Wi-Fi und Bluetooth. NFC-Tags sind billig und die Kommunikation mit ihnen bietet ein hohes Maß an Sicherheit, so dass in Zukunft mit einer stark anwachsenden Einsatzvielfalt zu rechnen ist. **ELV**



Bild 16: Erstaunlich, wie gut ein Verstärker mit 33 Jahren „auf dem Buckel“ mit moderner High-Tech harmoniert. Mit dem „AR 6103“ bekommt Musik vom Handy das Klangvolumen der Hi-Fi-Anlage.

