Elektrotechnik & Informationstechnik (2010) 127/5: 127–134. DOI 10.1007/s00502-010-0732-3

Eine mobile Service-Architektur für ein sicheres NFC-Ökosystem

G. Madlmayr, Ch. Kantner OVE, J. Scharinger, I. Schaumüller-Bichl

Das Mobiltelefon ist heute nicht mehr nur ein einfaches elektronisches Gerät, um mobil erreichbar zu sein. Durch die Integration zusätzlicher Technologien und leistungsfähiger Plattformen gibt es kaum Anwendungsdomänen, die vor dem Mobiltelefon halt gemacht haben. Das Telefon, das bereits heute das persönlichste aller Geräte für den Menschen ist, stellt ein digitales Abbild des Anwenders dar. Es repräsentiert dessen Kommunikation, Kontakte, Fotos, Musik und Anwendungen. Durch die Integration von kontaktloser Smartcard-Technologie unter der Bezeichnung Near Field Communication (NFC) wird diese Konzentration noch weiter verstärkt. Aus diesem Grund ist es erforderlich, entsprechende Sicherheitsmechanismen bereits bei der Integration von Anwendungen und Technologien zu berücksichtigen, was im Zuge dieser Arbeit genauer beleuchtet wird.

Der vorliegende Artikel beschäftigt sich mit einem Konzept und der Implementierung von Prototypen für die sichere Verwaltung von NFC-Anwendungen in einem Smartcardchip eines mobilen Endgerätes. Im Unterschied zu herkömmlichen Softwarekomponenten, die auf dem Applikationsprozessor des Telefons ausgeführt werden, laufen NFC-Anwendungen zur Simulation einer Smartcard in einem so genannten sicheren Element. Durch die Integration dieses sicheren Elements und der kontaktlosen Smartcard-Funktionalität entsteht im Grunde genommen eine Chipkarte mit einem Display, einem Keyboard und einer Netzwerkanbindung. Diese Komponenten nutzend, werden in dieser Arbeit unterschiedliche Ansätze vorgestellt, wie die Anwendungen im sicheren Element des Telefons über eine Datenverbindung fernverwaltet werden können. Durch das vorgestellte System können in Zukunft Chipkartenanwendungen in einer sicheren Art und Weise an ein Mobiltelefon übertragen werden, wodurch keine physischen Plastikkarten mehr als Trägermedium erforderlich sind.

Schlüsselwörter: Near Field Communication; Smartcard-Anwendungen; NFC-Ökosystem; OTA-Management

A mobile service architecture for a secure NFC ecosystem.

Modern mobile phones are more than just simple electronic devices for mobile communication. New hardware and software technology allow a great variety of application domains on devices today. People's mobile phones have become one of their most personal possessions: the contacts, photos, music, and applications are a digital representation of their owner. By the integration of contactless smartcard technology, also referred to as Near Field Communication (NFC), this concentration of personal information is strengthening. For this reason, safety and privacy mechanisms need to be considered before integrating new technology or applications into a device. What the appropriate mechanisms should be will be discussed in more detail in this work.

This article deals with the secure management of NFC applications in the smartcard chip of a mobile device, both conceptually and via a prototypical implementation. Of primary concern in this work are NFC applications for the emulation of smartcards, which run on the so-called secure element, in contrast to conventional software, which runs on the application processor of the telephone. Integrating a secure element and contactless smartcard functionality into a mobile device produces a smartcard with a display, a keyboard and a network connection. Using these components, it can be shown how applications in the secure element of a telephone can be managed through a data connection. The concepts presented can be used to overcome the need for physical plastic cards in the future, as the issuing process can be done via the mobile network.

Keywords: near field communication; smartcard-applications; NFC ecosystem; OTA management

Eingegangen am 18. Jänner 2010, angenommen am 1. April 2010

1. Einleitung

Technologien sind aus den unterschiedlichsten Bereichen des alltäglichen Lebens nicht mehr wegzudenken. Während allerdings der eine Teil bewusst als Technologie oder Gerät wahrgenommen wird (z. B. Mobiltelefon), gibt es auch jene, die so intuitiv verwendet werden können, dass sie vom Anwender nicht mehr als solche wahrgenommen werden (*Weiser, 1995*).

Ein Beispiel für Zweiteres sind die bereits weit verbreiteten kontaktlosen Chipkarten auf RFID-Basis, die für die Zutrittskontrolle bei Veranstaltungen, Freizeitparks und Skigebieten eingesetzt werden. Durch die Automatisierung des Kontrollprozesses kann nicht nur der Zugang effizienter gestaltet werden, sondern auch die Sicherheit der Tickets verbessert werden. Der Nutzer profitiert insofern von dem Einsatz dieser Technologie, als dass er nicht mehr mit langwierigen Kontrollprozessen konfrontiert ist, sondern diese beinahe unbemerkt durchgeführt werden. Entsprechende Maßnahmen zur Sicherung des Datenschutzes müssen in diesem Kontext berücksichtigt werden, um die Privatsphäre des Anwenders nicht zu verletzen.

Unter der Bezeichnung NFC (Near Field Communication) soll RFID-Technologie auch Einzug in elektronische Endgeräte des Endver-

Madlmayr, Gerald, Dipl.-Ing. (FH), Mobile Consulting Vienna, Gumpendorfer Straße 81/1/15, 1060 Wien, Österreich; **Kantner, Christian, Dipl.-Ing.,** mobilkom austria AG, Obere Donaustraße 29, 1020 Wien, Österreich; **Scharinger, Josef, A. Univ.-Prof. Dipl.-Ing. Dr.,** Johannes Kepler Universität, Institut für Computational Perception, Altenberger Straße 69, 4040 Linz, Österreich; **Schaumüller-Bichl, Ingrid, Univ.-Doz. Dipl.-Ing. Dr.,** FH OÖ Studienbetriebs GmbH, Campus Hagenberg, Softwarepark 11, 4232 Hagenberg, Österreich (E-Mail: gerald@madlmayr.at)

brauchers halten, damit unterschiedliche Geräte relevante Daten austauschen können. Denkbar wären so Bluetooth Pairing von Notebook und Telefon durch eine Berührung oder auch die Herstellung einer WiFi-Verbindung zwischen einer Kamera und einem Fernsehgerät, um die Bilder der Kamera ohne weiteres Zutun am Fernsehgerät anzeigen zu können. Speziell interessant ist die Integration von NFC in Mobiltelefone. Diese können nämlich auf diese Weise mehrere kontaktlose Chipkarten simulieren. Wie dies technisch realisiert werden kann und welche Stakeholder in den Prozess des Managements von Chipkartenanwendungen in einem Mobiltelefon involviert sind, wird im Folgenden aufgezeigt. Abschließend werden unterschiedliche Prototypen vorgestellt, die die Realisierbarkeit eines solchen Systems zeigen.

2. Near Field Communication

Mit der Entwicklung und Standardisierung von NFC wurden von den Stakeholdern unterschiedliche Ziele verfolgt. Auf technologischer Ebene sollte ein Standard geschaffen werden, der neben den bereits standardisierten ISO/IEC 14443-A/B Systemen auch jene von Sonys FeliCa abdeckt, da eine geplante Standardisierung von FeliCa als ISO 14443-C (bzw. –F) nicht umgesetzt werden konnte. Ein Hauptziel war es, NFC kompatibel zu bestehenden Infrastrukturen von kontaktlosen Smartcards zu halten, um Synergien nützen zu können. Durch NFC sollte eine Day-to-Day-Technologie geschaffen werden, die im Alltag an unterschiedlichen Stellen zum Einsatz kommt, ohne dass dadurch Kosten für den Anwender entstehen. Eine Prämisse war auch, dass die Interaktion einfach und intuitiv sein und der Anwender nicht durch Komplexität von der Verwendung abgeschreckt werden sollte.

Das Ergebnis der Standardisierung ist eine kontaktlose Übertragungstechnologie, die an den Standard der kontaktlosen Smartcards, konkret ISO/IEC 14443, angelehnt ist. NFC ist in ISO/IEC 18092 und ECMA 340 standardisiert. In diesen Standards sind sowohl die elektromagnetischen Eigenschaften als auch das Übertragungsprotokoll NFCIP-1 definiert. Über NFC können Daten in Form des NDEF (Near Field Communication Data Exchange Format) ausgetauscht werden, das vom NFC-Forum definiert und laufend erweitert wird (*NFC-Forum, 2006*).

NFC basiert auf physikalischer Ebene auf elektromagentischer Induktion, wie sie auch bei RFID-Systemen zum Einsatz kommt. Während abhängig vom Einsatz bei RFID unterschiedliche Frequenzen für die Übertragung zum Einsatz kommen, ist die Frequenz bei NFC mit 13,56 MHz festgelegt. Dadurch wird eine Kompatibilität zu den bestehenden Smartcardsystemen erreicht (*Rankl, Effing, 2002*).

Die Kommunikationsdistanz bei NFC ist auf wenige Zentimeter beschränkt, um ein NFC-Endgerät als haptisches Eingabemedium verwenden zu können, damit nur von Benutzern gewollte Aktionen ausgeführt werden. Nichtsdestotrotz ist NFC auf ähnliche Angriffe wie auch RFID anfällig. So ist beispielsweise das Relaying der Kommunikation ohne Weiteres auch bei dieser neuen Technologie möglich (*Hancke, 2006*).

2.1 Anwendungsmodi

Während die Rollenverteilung in klassischen Smartcardsystemen bzw. RFID-Systemen mit Lesegeräten (PCD, Proximity Coupling Devices) und Smartcards (PICC, Proximity Inductive Coupling Card) klar geregelt ist, ist die Situation bei NFC-Geräten etwas anders. Ein NFC-Gerät kann per se nämlich entweder als Initiator der Kommunikation auftreten oder im Target-Modus darauf warten, von einem Kommunikationspartner angesprochen zu werden. Für ein NFC-Endgerät ergeben sich dadurch unterschiedliche Anwendungsmodi, und zwar (Abb. 1):

- *PCD-Modus:* In diesem Fall agiert das NFC-Endgerät als Lesegerät, baut ein Feld auf und ist in der Lage, mit einem externen Transponder zu kommunizieren. Um die Rückwärtskompatibilität mit bestehenden Systemen zu erlangen, wird hierfür das Protokoll nach ISO/IEC 14443 verwendet. Das NFC-Forum hat zudem das Datenformat NDEF (NFC Data Exchange Format) definiert, welches einem Lesegerät erlaubt, strukturierte Informationen von einem Transponder auszulesen und eine zugehörige Aktion, wie beispielsweise das Öffnen einer URL in einem Webbrowser am Telefon, auszuführen.
- *PICC-Modus*: Das NFC-Endgerät agiert als Chipkarte und kann von einem externen Lesegerät als solche erkannt werden. Das Lesegerät kann dabei nicht unterscheiden, ob es sich um eine Chipkarte oder ein NFC-Endgerät in diesem Modus handelt. Die Emulation der Chipkarte kann entweder in Software realisiert werden, die am Applikationsprozessor des NFC-Endgeräts ausgeführt wird, oder aber durch einen zusätzlichen physikalischen Smartcardchip realisiert werden. Dieser Smartcardchip wird im Kontext von NFC auch als sicheres Element bezeichnet und kann in unterschiedlichen Ausführungen im Endgerät vorhanden sein. Möglichkeiten dafür sind eigens in das Endgerät fix integrierte Smartcardchips oder aber welche auf einem entfernbaren Trägermedium wie einer Speicherkarte oder einer SIM-Karte. Der PICC-Modus wird auch als Card Emulation bezeichnet. Card Emulation stellt das größte Potential für neue Anwendungen dar, vor allem deshalb, weil NFC-Geräte mit Card Emulation auch in Legacy-Systemen, die ISO/IEC 14443-kompatibel sind, eingesetzt werden können, ohne dass das Infrastruktursystem an sich verändert werden muss. Anwendungsfälle dafür sind das Bezahlen sowie der Einsatz im öffentlichen Personennahverkehr.
- *NFC-Modus*: Durch den NFC-Modus könnten zwei NFC-Endgeräte bidirektional miteinander sprechen. Dieser Modus stellt einen grundsätzlich anderen Kommunikationsablauf dar als bei RFID-Systemen vorgesehen, weshalb dafür auch ein eigenes Protokoll, das

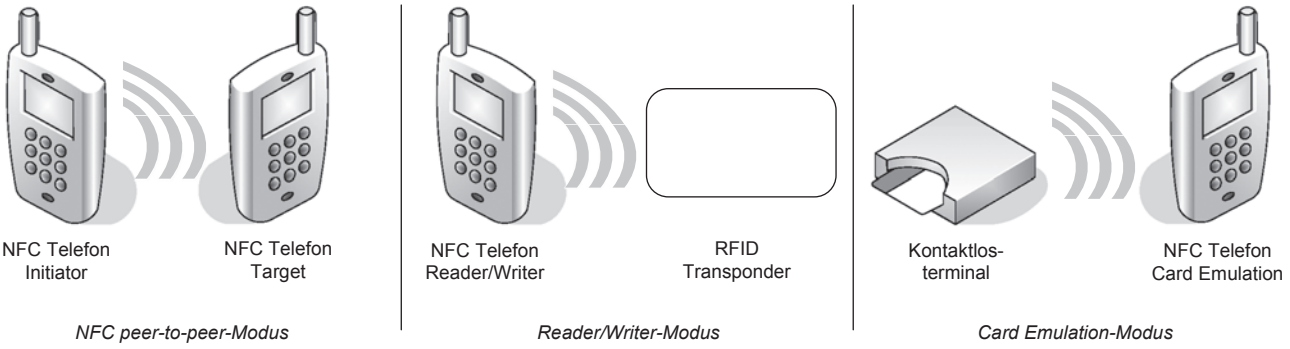

Abb. 1. Anwendungsmodi von NFC-Geräten

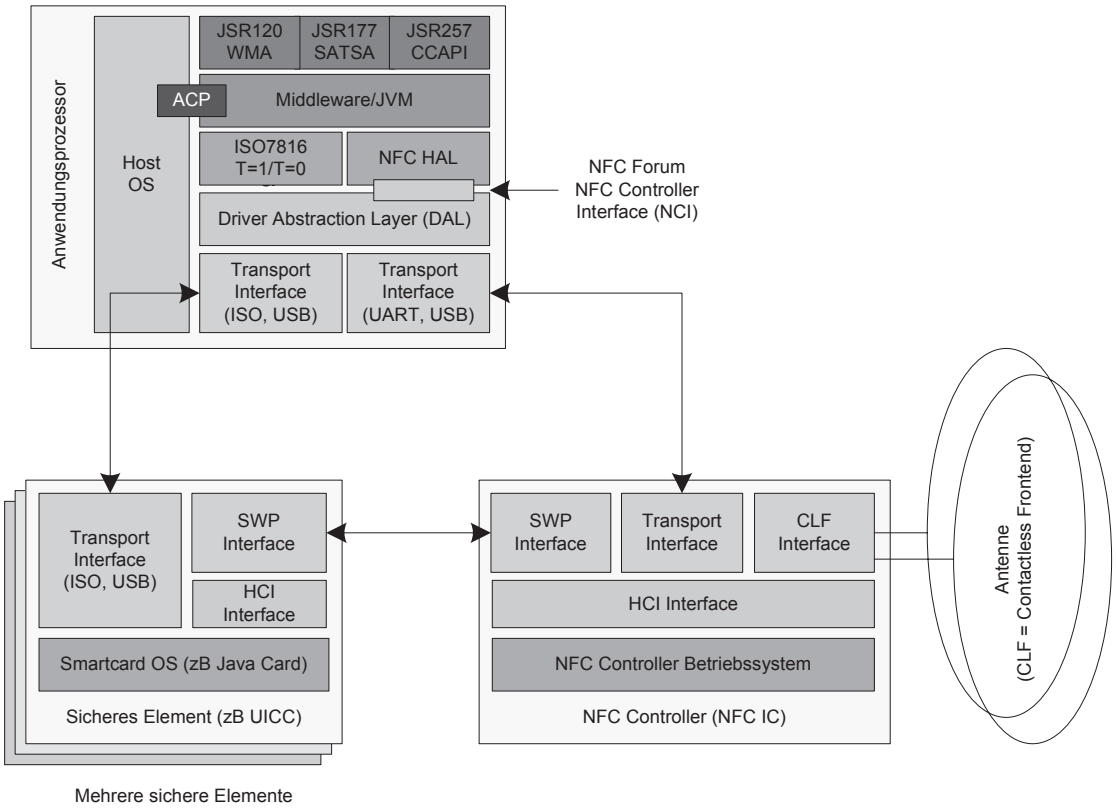

Abb. 2. Architektur für die Integration von NFC in ein mobiles Endgerät

NFCIP-1, entwickelt wurde. Der Vorteil dieser NFC-P2P-Verbindung gegenüber Bluetooth oder WiFi ist der rasche und automatisierte Aufbau der Verbindung (<0,5 Sekunden). Ähnlich wie beim PCD-Modus kommt auch hier NDEF zum Einsatz, um Daten zwischen den beiden Geräten auszutauschen. Das NFC-Forum hat für diesen Anwendungsmodus beispielsweise Formate definiert, um Visitenkarten durch eine Berührung von zwei Mobiltelefonen auszutauschen oder um zwei Geräte einfach über eine weitere Drahtlostechnologie wie Bluetooth, WiFi oder Wireless USB zu verbinden (*Fischer, 2009*).

2.2 Integrationsmöglichkeiten von NFC

Die Integration von NFC-Funktionalität in ein Mobiltelefon erfolgt in den aktuell verfügbaren Modellen in Form von Mehrchiplösungen, welche aus Applikationsprozessor, NFC-Controller und einem oder mehreren sicheren Elementen bestehen, wie in Abb. 2 dargestellt (*GSMA, 2007a*).

Sicheres Element: Das sichere Element kann in Form einer oder mehrerer Instanzen im Endgerät vorhanden sein. Gegenüber dem Applikationsprozessor ist das sichere Element immer Host und antwortet nur auf eingehende Anfragen. Die Schnittstelle hierfür ist ISO/IEC 7816, und die Kommunikation erfolgt über das $T=0$ bzw. $T=1$ Protokoll und APDUs. Das sichert die Kompatibilität zur SIM-Karte, die dieselbe Schnittstelle bietet. Neben dem ISO/IEC-Interface wird in Zukunft auch verstärkt eine USB-Schnittstelle vorzufinden sein, die eine breitbandige Verbindung zwischen sicheren Elementen und mobilem Endgerät zulässt. Auf Anwendungsebene (Java) steht die JSR177 zur Verfügung, um mit dem sicheren Element zu kommunizieren.

Zur Kommunikation mit dem NFC-Controller muss das sichere Element eine *Single Wire-Schnittstelle* (SWP) bereitstellen, über die durch das *Host Controller Interface* (HCI) definierte Daten zwischen den Kommunikationsteilnehmern gesendet werden können. Diese Schnittstelle erlaubt auch die Kommunikation zwischen zwei sicheren Elementen. Zum NFC-Controller hin ist das sichere Element ein Client, der bis auf wenige Kommandos (z. B. Loop-Back) allerdings aus Sicherheitsgründen nicht zu einer Kommunikation bewegt werden kann.

Anwendungsprozessor: Der Anwendungsprozessor übernimmt gegenüber dem NFC-Controller und dem sicheren Element die Rolle eines Client. Das sichere Element wird über das ISO/IEC 7816 oder USB Interface angesprochen, während die Kommunikation zum NFC-Controller über ein serielles Interface erfolgt und auf Protokollebene ebenfalls HCI zum Einsatz kommt. Der Anwendungsprozessor kann dem NFC-Controller bestimmte Events mitteilen, bei deren Auftreten der NFC-Controller einen Call-Back zum Anwendungsprozessor senden soll. Auf Anwendungsebene wird für die Ansteuerung die JSR257 verwendet.

NFC Controller: Der NFC Controller ist über drei verschiedene Schnittstellen (SWP, serielles Interface, kontaktloses Interface) jeweils als Host zu erreichen, wobei mit Ausnahme der kontaktlosen Schnittstelle auch hier HCI zum Einsatz kommt. Für die drahtlose Kommunikation werden aus Kompatibilitätsgründen ISO/IEC 14443 (APDUs), ISO/IEC 18092 (Logical Link Control Protocol, LLCP) und FeliCa (F-Frames) eingesetzt.

Diese Architektur bildet auch die technische Grundlage für diese Arbeit.

3. Architektur für Over-the-Air (OTA) Management

Durch die Integration von NFC-Technologie in ein Mobiltelefon ergeben sich interessante Möglichkeiten für Smartcard-Anwendungen. Da das Endgerät auch automatisch ein Terminal für das sichere Element darstellt, erhält der Smartcardchip dadurch ein Display

und ein Keyboard zur Interaktion sowie eine Netzwerkanbindung, um Daten mit zentralen Komponenten auszutauschen. Dadurch ist es möglich, dass Anwendungen erst nach der Ausgabe des sicheren Elements installiert und personalisiert werden. Dies erlaubt es, Daten für den Endverbraucher erst bei Bedarf und individuell auf dem sicheren Element einzurichten, ohne dass der Endverbraucher das mobile Endgerät aus seinen Händen gibt. Dies stellt einen zentralen Vorteil gegenüber klassischen Smartcardsystemen bzw. CAMS (Card Application Management-Systemen) dar. Hinzu kommt, dass der Smartcardchip in der Lage ist, mehrere unterschiedliche Smartcard-Anwendungen zu beherbergen.

Für sichere Elemente in mobilen Endgeräten haben sich JavaCard OS-basierende Chips mit dem GlobalPlatform Framework (*GlobalPlatform, 2010*) zur Anwendungsverwaltung als Quasi-Standard durchgesetzt. Zusätzlich sind auch Systeme wie NXPs MIFARE als auch Sonys FeliCa zu berücksichtigen, um eine breite Rückwärtskompatibilität mit bestehenden Infrastruktursystemen von kontaktlos arbeitenden Lesegeräten zu erlauben.

3.1 Rollen

Innerhalb des Systems gibt es unterschiedliche Rollen, die unterschiedliche Aufgaben übernehmen. Abhängig von den wirtschaftlichen sowie den rechtlichen Gegebenheiten könnten diesen Rollen von einem oder mehreren Marktteilnehmern eingenommen werden. Da dieses System auch einer gewissen Dynamik unterliegt, wird auch von einem Ökosystem gesprochen (*GSMA, 2007b*).

Folgende Rollen sind in dem Ökosystem für die Fernverwaltung erforderlich (Abb. 3):

- Plattform Provider: Der Plattform Provider (PP) stellt die ausgebende Stelle des sicheren Elements dar. Für den Fall, dass das sichere Element in der SIM-Karte untergebracht wird, ist der Mobilfunknetzbetreiber der Plattform Provider; ist das sichere Element fix in das Endgerät integriert, agiert der Telefonhersteller als Plattform Provider; kommen sichere Speicherkarten zum Einsatz, agieren die entsprechenden ausgebenden Stellen als Plattform Provider. Dabei kann es sein, dass der Plattform Provider auch selbst Anwendungen auf dem sicheren Element unterbringen möchte und somit als Service Provider agiert. Der Mobilfunknetzbetreiber mit seiner GSM/USIM-Anwendung ist ein Beispiel dafür. Die Verwaltung der Anwendungen auf dem sicheren Element wird an den Plattform Manager abgetreten.
- Service Provider: Der Service Provider (SP) stellt Dienste bereit, die es erfordern, dass Daten und Anwendungen im sicheren Element liegen bzw. abgelegt werden. Dazu wird jedem Anwendungsanbieter ein Bereich im sicheren Element zugewiesen, in dem seine Anwendung untergebracht wird. Der Service Provider muss sich allerdings nicht selbst um die Verwaltung der Anwendung kümmern – dies wird vom Plattform Manager übernommen.
- Plattform Manager: Der Plattform Manager (PM), auch Trusted Service Manager (TSM) genannt, kümmert sich um die Verwaltung des sicheren Elements sowie des Lebenszyklus der darauf untergebrachten Anwendungen. Der Plattform Manager dient dazu, die *n*-zu-*m*-Relation zwischen ausgebenden Stellen bzw. deren sicheren Elementen und Anwendungsanbietern aufzulösen. Technisch ist es auch möglich, dass ein sicheres Element in mehrere Bereiche aufgeteilt ist, die von unterschiedlichen Plattform Managern verwaltet werden. Neben der Verwaltung von Anwendungen in den sicheren Elementen der mobilen Endgeräte kann der Plattform Manager auch die Kundenbetreuung (Customer Care), die Bestellung von sicheren Elementen (Order Management), die Prüfung und Zertifizierung von Anwendungen oder auch die Bereitstellung einer Key Management-Infrastruktur für die Plattform und Service Provider übernehmen.

Neben diesen organisatorischen Rollen sind auch zwei technische Komponenten erforderlich: einerseits der Mobilfunknetzbetreiber, der eine Datenverbindung und SMS-Funktionalität bereitstellt, sowie eine Verwaltungseinheit am Endgerät, die eine Brückenfunktion zwischen Plattform Managern und sicheren Elementen darstellt. Auf mögliche Implementierungsmöglichkeiten der Verwaltungseinheiten wird in Abschnitt 4 genauer eingegangen.

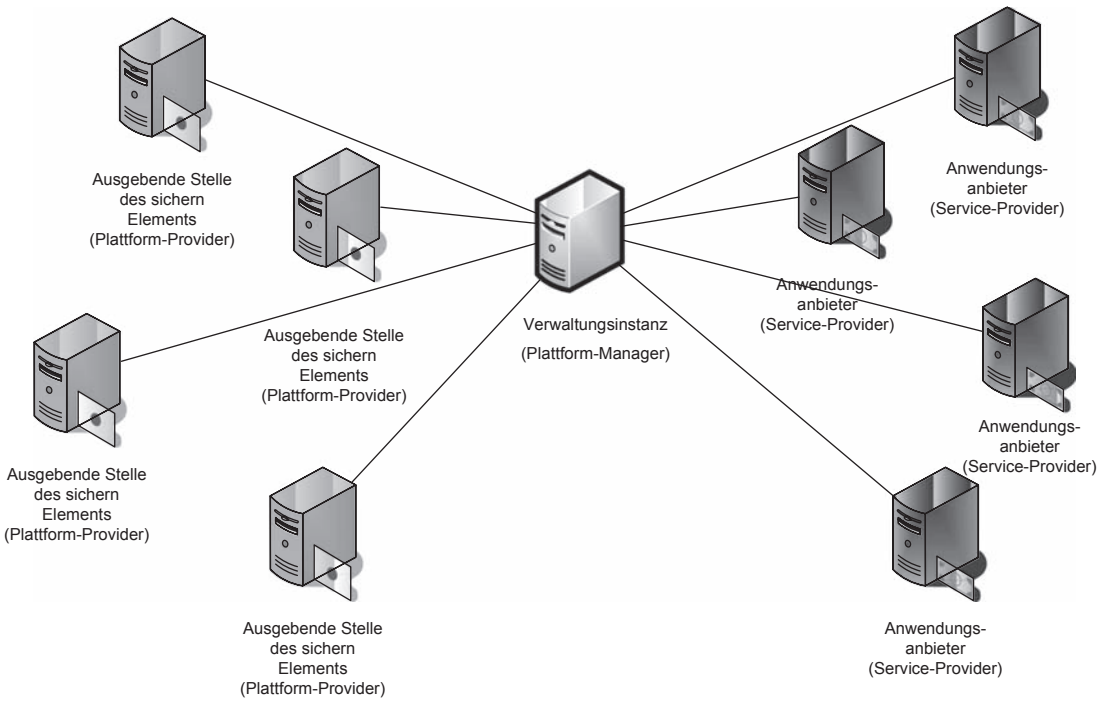

Abb. 3. NFC-Ökosystem

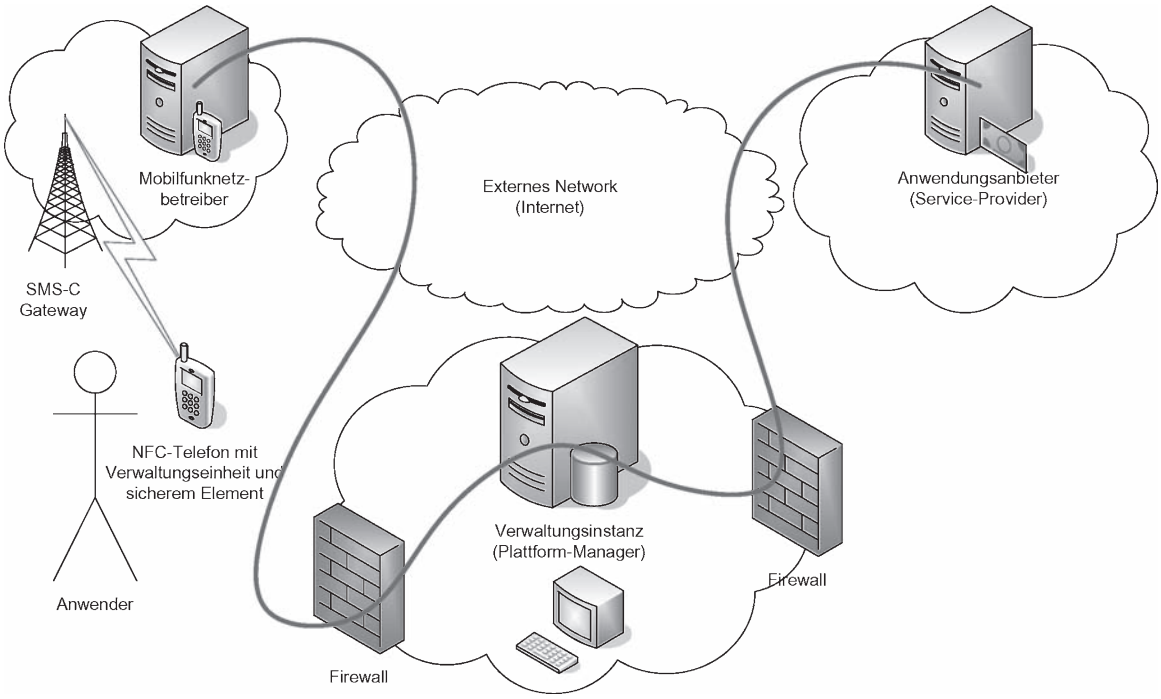

Abb. 4. Prozess des OTA-Managements in einem Mobilfunknetz

3.2 OTA-Management

Für das Over-the-Air (OTA)-Management ist es erforderlich (Abb. 4), dass zwischen dem sicheren Element und dem Backendsystem eine Datenverbindung hergestellt wird. Da üblicherweise ein Mobiltelefon keine fixe Adresse in einem IP-Netzwerk besitzt, ist es notwendig, dass der Verbindungsaufbau vom Telefon zum Backend hin geschieht. Dafür gibt es drei unterschiedliche Mechanismen:

- Der Anwender weist das Endgerät von sich aus an, eine Verbindung herzustellen, um beispielsweise eine Smartcardanwendung herunterzuladen. Diese Methodik wird beim Browser-basierenden Ansatz, wie in Abschnitt 4.1 beschrieben, angewendet.
- Das Telefon verbindet sich zeitgesteuert (z. B. alle 72 Stunden) mit dem Backendsystem und sieht sich nach möglichen Aktualisierungen bzw. für den Anwender verfügbaren Anwendungen um.
- Das Telefon wird über eine SMS darauf hingewiesen, dass eine neue Anwendung verfügbar ist und baut daraufhin die Verbindung zum Server auf. Diese Lösung ist für mobile Endgeräte der gangbarste Ansatz, da eine automatisierte und echtzeitfähige Lösung realisiert werden kann. Diese Implementierung kommt auch bei den Implementierungen für das MIDlet sowie dem SIM-basierenden Ansatz zur Anwendung (siehe Abschnitte 4.2 und 4.3).

4. Verwaltungseinheit

Die Verwaltungseinheit kümmert sich um die Herstellung der Verbindung zwischen Smartcardchip und Backendsystem. Abhängig vom verwendeten sicheren Element ergeben sich unterschiedliche Möglichkeiten für die Umsetzung.

4.1 Webbrowser-basierender Ansatz

Die erste der drei Implementierungen (Abb. 5) erlaubt das Management eines NFC-Targets, welches entweder durch ein Telefon im *Card Emulation*-Modus oder eine Smartcard repräsentiert werden kann. Dieser Ansatz unterscheidet sich von den beiden folgenden vor allem in zwei Punkten: Erstens kommt kein mobiles Endgerät als Terminal zum Einsatz, sondern ein PC mit einem Smartcard-Lesegerät, und zweitens werden keine Kurzmitteilungen zur Signalisierung verwendet.

Die gesamte Kommunikation zwischen dem Terminal und dem Managementsystem läuft über ein IP-basierendes Netzwerk, klassischerweise über das Internet. Durch die Umsetzung eines Pull-Konzepts, bei dem sich der Client selbständig zum Server verbindet, muss nicht auf die Signalisierung via SMS, ein Push-Konzept, zurückgegriffen werden. Durch den Verzicht auf die Kurzmitteilungen entfällt die Möglichkeit der Aktivierung und Deaktivierung des sicheren Elements via SMS im Falle von Diebstahl oder Verlust. Dafür wird allerdings die Möglichkeit gewonnen, auch Smartcards, die per se über keine Netzwerkanbindung verfügen, verwalten zu können.

Vor allem bereits existierende Smartcardlösungen könnten von diesem System profitieren, da keine Adaptierung für ein Mobilfunknetz vorgenommen werden muss. Das System kann auch vice versa genützt werden, um beispielsweise Bezahlungen im Internet über ein NFC-Target durchzuführen. Im Fall von Kreditkartentransaktionen könnte der Onlineshop sicherstellen, dass der Käufer auch tatsächlich im Besitz der physischen Karte bzw. des Telefons ist, und nicht nur der Kartennummer und des Sicherheitscodes.

Die Verwendung von einfachen PCs mit Internetverbindung als Terminal ermöglicht die Nutzung des Service durch eine Vielzahl von Teilnehmern ohne großen Aufwand. Neben dem Management von Anwendungen bieten sich auch vielversprechende neue Interaktionsmöglichkeiten mit Webanwendungen durch kontaktlose Karten an. Leider stellt die Nutzung eines offenen Systems mit vielen unterschiedlichen Komponenten auch eine beträchtliche Gefahrenquelle dar. Hinzu kommt der Aufwand durch die Installation der Verwaltungseinheit durch den Benutzer und die Verwendung von zusätzlicher Hardware (externes Lesegerät), die wiederum einen eigenen Treiber benötigt. Dies sind Hemmnisse für die Einführung einer solchen Lösung.

4.2 J2ME-Implementierung

In diesem Fall wird die Verwaltungseinheit in Form eines *MIDlets* realisiert, das direkt am Mobiltelefon läuft (Abb. 6). Für die Kommu-

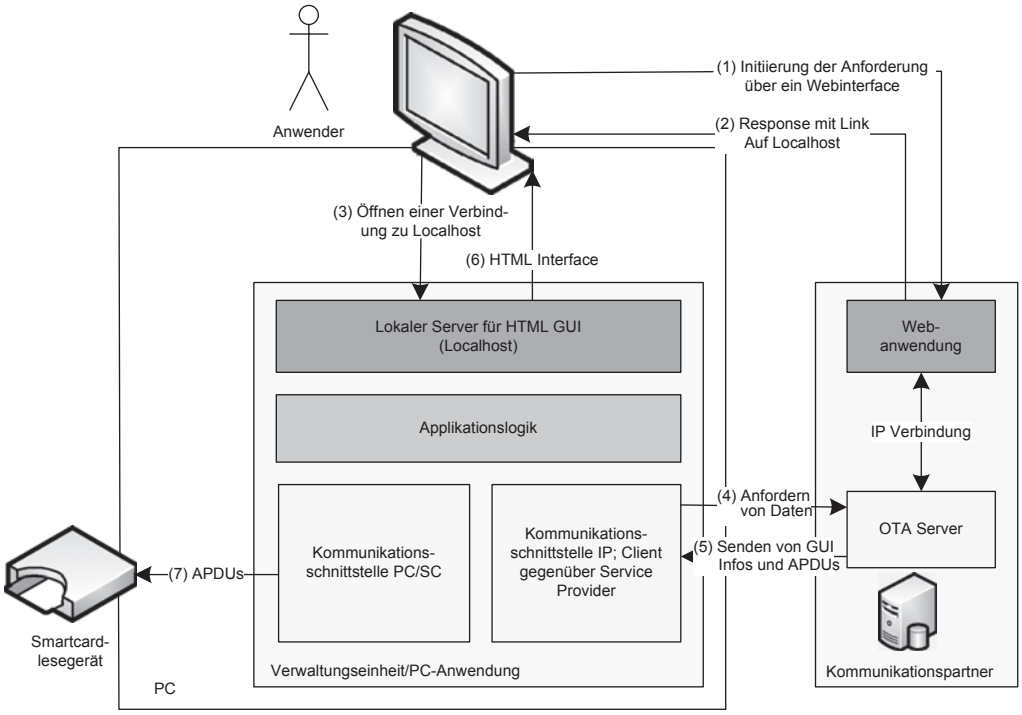

Abb. 5. Webbrowser-basierender Ansatz

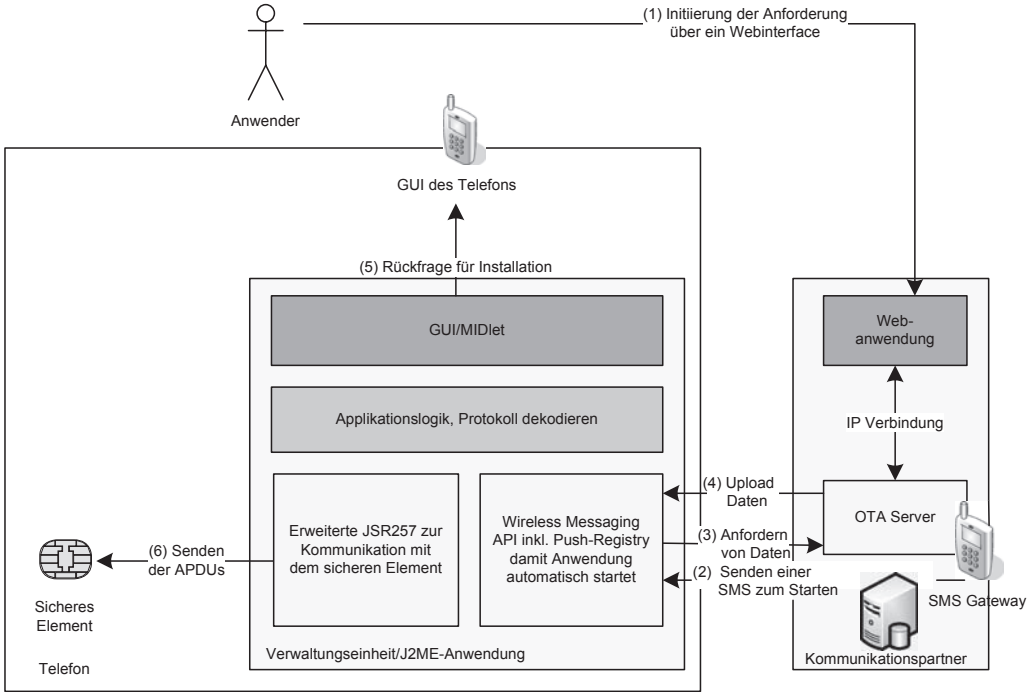

Abb. 6. MIDlet-basierender Prototyp

nikation mit dem sicheren Element bedient sich das MIDlet der *Secury Application and Trusted Service API* (*SATSA, JSR177*), die es erlaubt, *Application Protocol Data Units* (APDU) zur Kommunikation mit dem Smartcardchip über diese Schnittstelle zu senden. Um zu verhindern, dass jede beliebige Anwendung aus der Java Sandbox am Telefon auf die sicheren Elemente zugreifen kann, wird die Schnittstelle durch den *Access Condition Policy Enforcer* (ACP) überwacht. Somit ist es nur Java-Anwendungen mit einer entsprechenden Signatur möglich, auf das sichere Element zuzugreifen und Daten auszutauschen. Dieses ist allerdings nur eine Softwareimplementierung und kann umgangen werden, wie in (*Gowdiak, 2004*) gezeigt wurde.

Die J2ME-Implementierung kann auch eingesetzt werden, um so genannte NFC-Sticker zu verwalten, die über Bluetooth mit dem Telefon sprechen (*Twinlinx, 2009*). In diesem Fall wird die entsprechende API, die JSR82, zur Kommunikation herangezogen, wobei anzumerken ist, dass für diese Schnittstelle kein Berechtigungskonzept wie bei der JSR177 vorgesehen ist.

Für die Kommunikation mit dem Backendsystem wird die Wireless Messaging API (*WMA, JSR120*) eingesetzt. Der Plattform-Manager ist so in der Lage, eine Kurzmitteilung an das MIDlet zu senden, mit der Information, dass sich dieses beim Plattform-Manager melden muss. Das MIDlet am Telefon verifiziert die Authentizität der Kurzmitteilung und kontaktiert daraufhin den Plattform-Manager, der somit in der Lage ist, aus der Ferne das sichere Element durch das MIDlet zu verwalten.

Der Ansatz stellt eine gangbare Lösung für aktuell verfügbar Mobiltelefone mit NFC-Technologie dar, wie das Nokia 6216 oder das Sagem my700X. Allerdings verfügen im Moment noch kaum Mobiltelefone über eine Implementierung der JSR177, die für das OTA-Management vital ist. Problematisch ist, dass das MIDlet immer unter der Kontrolle des Anwenders ist. Dadurch kann das MIDlet vom Anwender auch vom Telefon entfernt werden oder der Prozess des OTA-Managements nach Belieben unterbrochen werden.

4.3 SIM-Karten-basierender Ansatz

Im Zuge dieses Ansatzes wurde die Verwaltung von Anwendungen durch einen Client, der direkt auf der SIM-Karte läuft, evaluiert (Abb. 7). Vorweg sei angemerkt, dass im Moment noch keine SIM-Karten erhältlich sind, die ein solches OTA-Anwendungsmanagement nach GlobalPlatform erlauben, weshalb die Funktionalität dieses Prototypen gegenüber den beiden vorherigen Ansätzen eingeschränkt ist.

Die Implementierung der Verwaltungseinheit erfolgt in diesem Fall als JavaCard-Anwendung, die direkt auf der SIM-Karte ausgeführt wird. Dadurch lässt sich zwar nur die SIM-Karte verwalten, allerdings entfällt das Installieren von zusätzlichen Komponenten am Endgerät. Des Weiteren läuft im Gegensatz zu den beiden anderen Implementierungen die Verwaltungseinheit im Smartcardchip und somit in einer gut geschützten Umgebung.

Konzeptionell verhält sich die Verwaltungseinheit auf der SIM-Karte so wie die Java-Implementierung am Mobiltelefon. Die Anwendung wird durch eine SMS mit einem speziellen TAR (Target Application Referer) vom Plattform-Manager angestoßen. Die Verwaltungseinheit prüft die SMS auf Authentizität und baut daraufhin eine Datenverbindung über BIP (Bearer Independent Protocol) zum Plattform-Manager auf. Durch das BIP kann die SIM-Karte das Telefon anweisen, Kommunikationsverbindungen über verschiedene Kanäle zu öffnen, wodurch es auch möglich ist, eine IP-Verbindung direkt von der SIM-Karte weg aufzubauen. Das BIP stellt eine zentrale technische Komponente dar, die für die Realisierung einer IP-Verbindung zwischen der SIM-Karte und einer externen Komponente notwendig ist.

Diese Implementierung kann mit zwei entscheidenden Vorteilen aufwarten: Die Kommunikation ist sicherer, weil Zertifikate und Schlüssel für die Kommunikation direkt im Smartcardchip abgelegt werden können und zudem auch die Kommunikation direkt von der SIM-Karte initiiert wird und für den Anwender nicht beeinflussbar ist. Zudem ist diese Implementierung unabhängig vom Betriebssystem des Endgerätes. Auch muss beim Wechsel des Endgerätes die Verwaltungseinheit auf dem neuen Endgerät nicht erneut installiert werden.

In Hinblick auf eine sichere Verwaltungseinheit ist die SIM-basierende Lösung der optimale Weg. Die fixe Bindung der Verwaltungs-

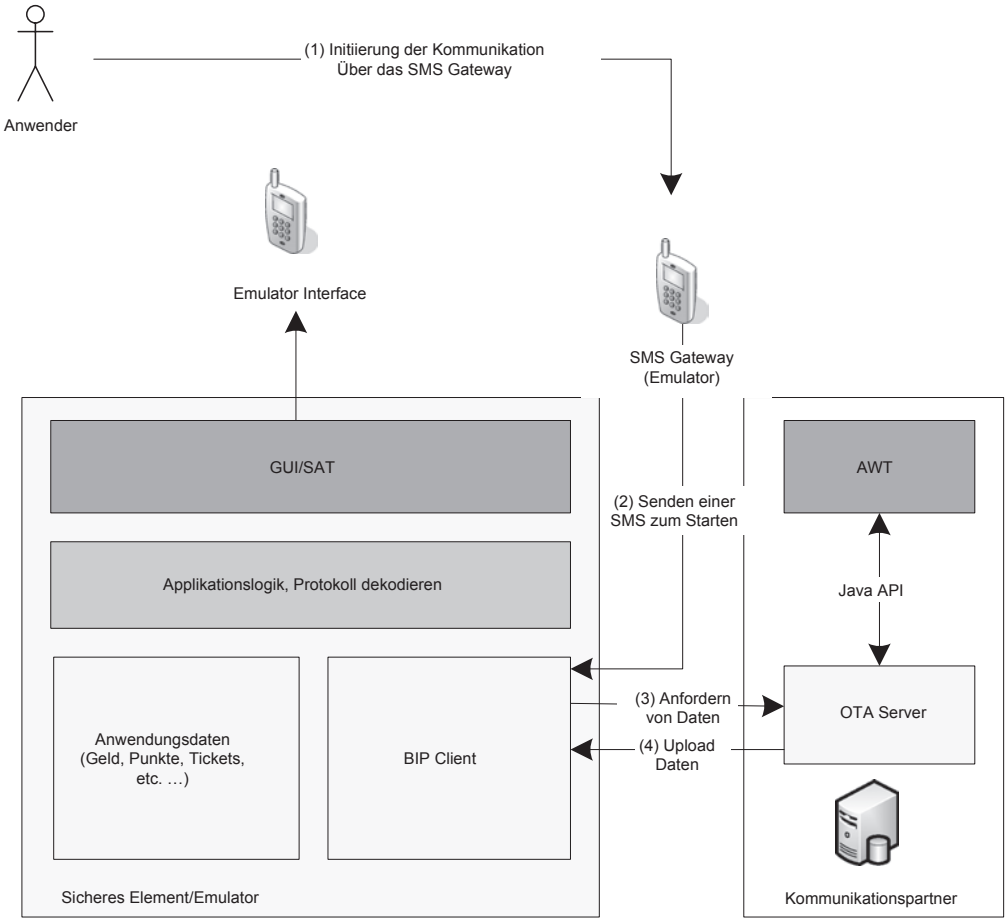

Abb. 7. SIM-Karten-basierender Ausatz

einheit an die MSISDN sowie die Integration in einen Smartcardchip ist bei den beiden anderen Lösungen nicht gegeben. Angriffe auf Verfügbarkeit und Integrität dieser Lösung sind am aufwändigsten zu realisieren, sie bietet daher die größte Sicherheit der drei Implementierungen.

5. Zusammenfassung

Kontaktlostechnologie wird in absehbarer Zeit in mobile Endgeräte für unterschiedliche Anwendungsfälle wie Bezahlen oder Ticketing im öffentlichen Personennahverkehr Einzug halten. In diesem Kontext werden OTA-Transaktionen sowie das Management des sicheren Elements eine zentrale Rolle spielen. Für diesen Anwendungsfall ist Client-seitig eine Softwarekomponente erforderlich, die eine Brücke zwischen den sicheren Elementen und dem Managementsystem herstellt. In der Arbeit wurden unterschiedliche Implementierungen sowie deren Vor- und Nachteile aufgezeigt. Die wahrscheinlichste Implementierung stellt eine Realisierung auf Basis bzw. eine Integration in die SIM-Karte dar. Im Moment arbeitet auch das Industrie-Gremium GlobalPlatform an den entsprechenden Spezifikationen.

Literatur

Fischer, J. (2009): NFC in cell phones: the new paradigm for an interactive world. Communication Magazine, IEEE 47 (6): 22–28.

GlobalPlatform (2010): Technical Overview, http://www.globalplatform.org/specifications.asp/.

Gowdiak, A. (2004): Java 2 Micro Edition (J2ME) Security Vulnerabilities. Proc. of the Hack in the Box Security Conf.

GSMA (2007a): Mobile NFC technical guidelines v2.0, White Paper.

GSMA (2007b): Mobile NFC Services, White Paper.

Hancke, G. (2006): A practical relay attack on ISO 14443 proximity cards. Symp. on Security and Privacy.

NFC-Forum (2006): NDEF Specifications, http://www.nfc-forum.org/specs/.

Rankl, W., Effing, W. (2002): Handbuch der Chipkarten – Aufbau, Funktionsweise und Einsatz von Smartcards. München: Carl Hanser.

Twinlinx (2009): Mobile NFC Sticker MyMax, http://www.twinlinx.com/.

Weiser, M. (1995): The Computer for the 21st Century. San Francisco: Morgan Kaufmann Publishers.

Autoren

Gerald Madlmayr
arbeitet als IT-Berater mit Schwerpunkt Telekommunikation in Wien. Dabei behandelt er Themen im M-Commerce-Bereich mit Fokus auf neue Technologien und Sicherheit. Zuvor war er vier Jahre als wissenschaftlicher Mitarbeiter am Campus Hagenberg der FH OÖ tätig und beschäftigte sich mit NFC/RFID-Technologie für mobile Systeme. Im Zuge seiner Tätigkeit wurde der erste NFC-Feldversuch in Österreich realisiert. Seine Arbeit spiegelt sich zudem in mehr als 15 Publikationen zum Thema NFC wieder.

Christian Kantner
Nach Abschluss seines Elektrotechnikstudiums an der Technischen Universität Wien 1997 war Christian Kantner für die Architektur und die Implementierung von Daten und Fax-Protokollen für ein Satellitentelefonsystem verantwortlich. Dabei war er für Ascom Switzerland und Hughes Network Systems in den USA tätig. 2003 wechselte Christian Kantner in das Techlab von mobilkom austria. Er beschäftigte sich dort mit neuesten Entwicklungen im Bereich mobiler Endgeräte und startete seine NFC-Aktivitäten 2004. Christian Kantner ist Co-Editor der NFC technical guidelines der GSMA. Seit 2007 ist Christian Kantner für NFC-Agenden im Produkt Management von mobilkom austria zuständig.

Josef Scharinger
promovierte 1995 an der Johannes Kepler Universität Linz und ist an dieser derzeit als Außerordentlicher Universitätsprofessor am Institut für Computational Perception tätig. Er fungiert laufend als Gutachter für eine Vielzahl von internationalen Journalen und Tagungen und hat mehr als 60 internationale wissenschaftliche Publikationen in Büchern, Journalen und Tagungsbänden veröffentlicht. Des Weiteren ist er Mitverfasser von vier Patenten im Gebiet der IT-Sicherheit.

Ingrid Schaumüller-Bichl
studierte Technische Mathematik an der Johannes Kepler Universität Linz. 1992 erfolgte die Habilitation im Fach ,,Angewandte Informatik'' an der Universität Klagenfurt.

Frau Dr. Schaumüller-Bichl ist seit mehr als 20 Jahren im Bereich IT-Sicherheit in Forschung, Entwicklung und Consulting tätig. Nach mehreren Jahren als Leiterin der Entwicklung von Sicherheitssystemen in der Industrie und anschließend als selbständige Unternehmensberaterin für das Fachgebiet IT-Sicherheit mit umfangreicher internationaler Forschungs-, Entwicklungs- und Vortragstätigkeit übernahm Dr. Schaumüller-Bichl 2006 eine Professur für Sicherheits- und Risikomanagement an der FH OÖ Campus Hagenberg. Seit 2008 ist sie auch Vizedekanin für Forschung und Internationalisierung der Fakultät für Informatik, Kommunikation und Medien in Hagenberg.

Dr. Schaumüller-Bichl ist weiters Lehrbeauftragte an den Universitäten Linz, Klagenfurt und Krems, Vizepräsidentin der OCG, österreichische Repräsentantin in IFIP TC11 sowie Mitglied des Rates für Forschung und Technologie Oberösterreich (RFT OÖ).

