Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Sichere Infrastruktur zur Fernverwaltung von Smartcard-Chips in einem NFC- Ökosystem

Gerald Madlmayr

NFC Research Lab, Hagenberg

D*A*C*H Security – 25. Juni 2008

www.nfc-research.at

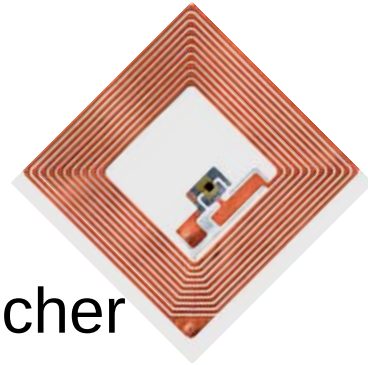
mobilkom austria

OMNIKEY

NXP founded by Philips

TU WIEN

Was ist NFC?



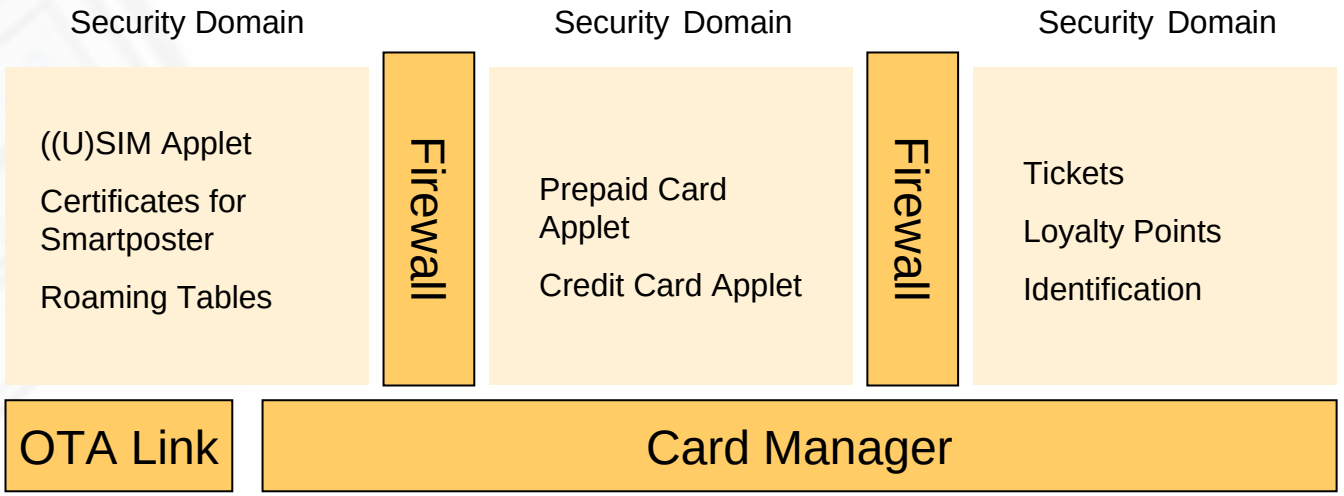
- RFID Derivat, 13,56 Mhz
- Integration in mobile Endgeräte für Endverbraucher
- Reichweite: 0 – 10 cm
  (proximity Technologie)
- Ziel: Einfache Interaktion

NFC Devices: Anwendungsmodi

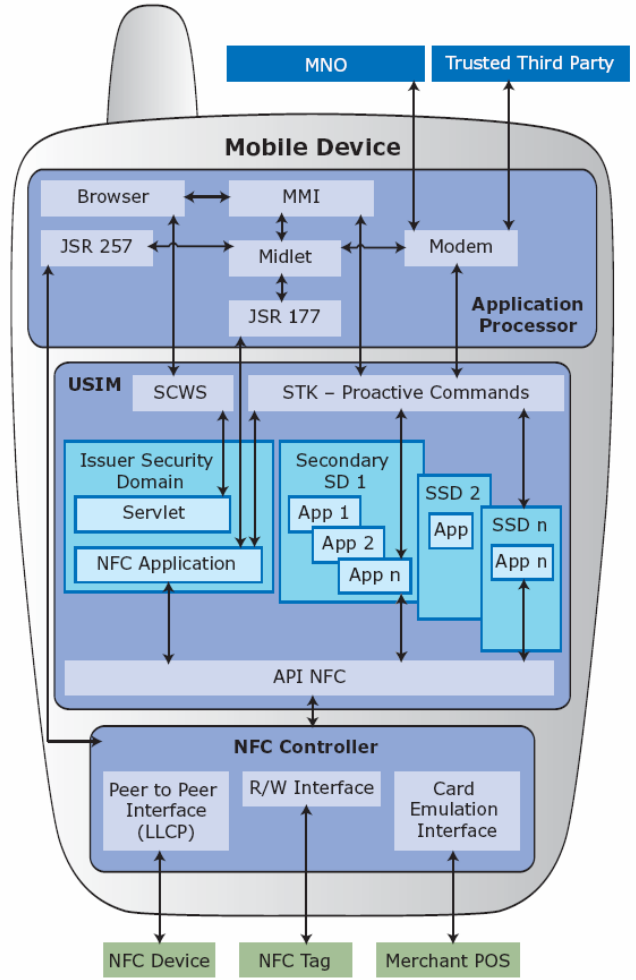
- Bidirektionaler Modus (P2P – NFC peer-to-peer)
  - Bidirektionale Verbindung um Daten auszutauschen (ISO18092)
  - WiFi, BT, P2P Payment, Contacts, vCards, …
- Lese/Schreib Modus (PCD – Proximity Coupling Device)
  - Lesegerät für RFID/Smartcard Tags (ISO14443)
  - SmartPoster, WiFi Config, Ring-Tones, …
- Emulation von Smartcards (PICC – Proximity Card)
  - Externes Lesegerät kann zw. Smartcard/Mobiltelefon nicht unterscheiden
  - Mehrere Smartcards im Telefon abgebildet

Multi Applications Card

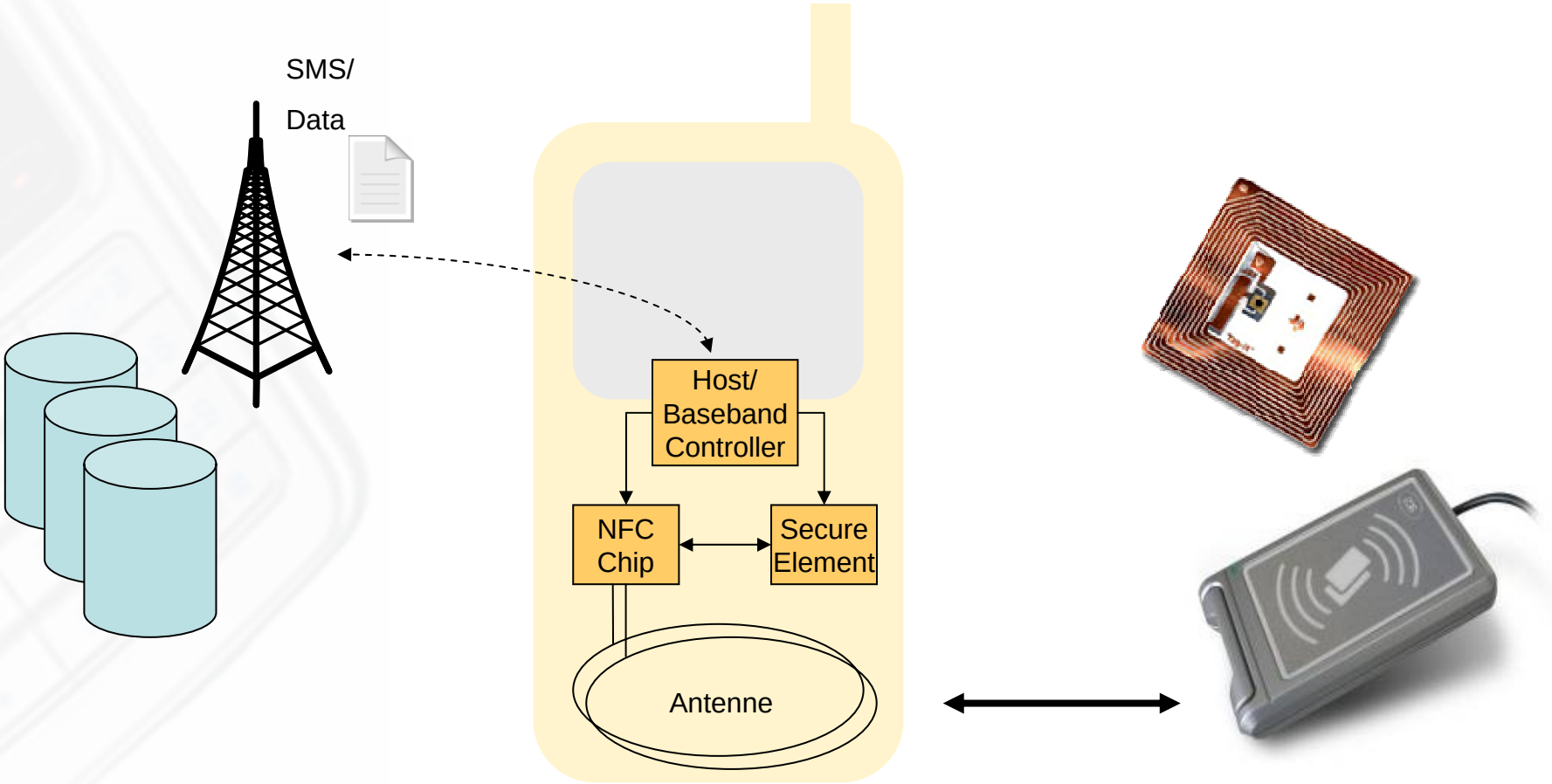
- Card Emulation
  - Smartcard Anwendungen werden auf „Software“ reduziert
  - Ausgabe der Karte durch Ausgabe von Software ersetzt.
  - Ein oder mehere „sichere Elemente“ im mobilen Endgerät
  - => Netzwerk, Bildschirm, Tastatur für Smartcard



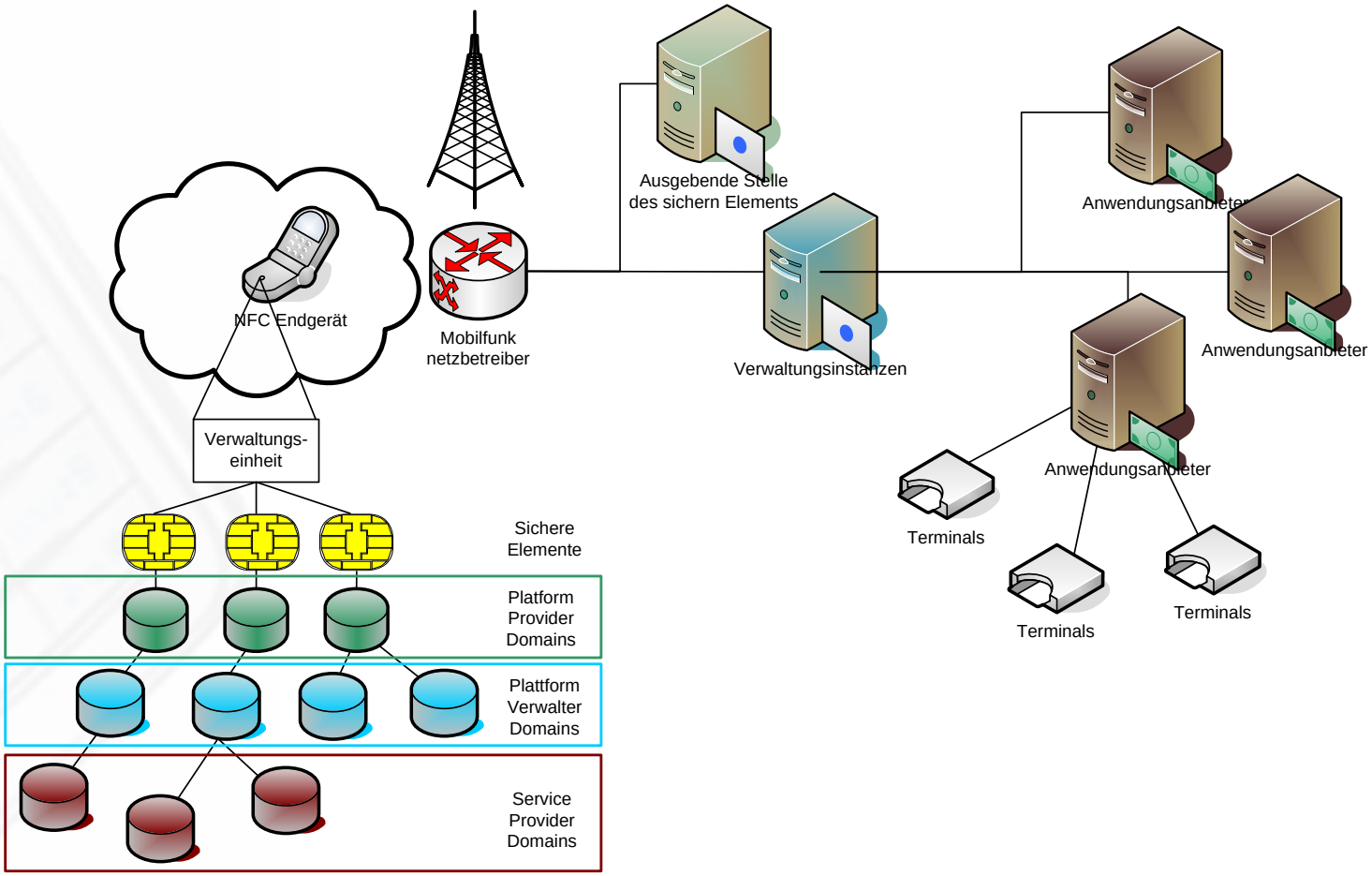
NFC Device Architecture



NFC Devices: Bridging the Gap



System für Fern-Verwaltung von Smartcard Applikationen



Veraltung

- Initialisierung der PKI
- Personalisierung des sicheren Elements (vor der Ausgabe)
- Ausgabe des sicheren Elements
- Erweiterte Personalisierung durch Plattform Manager
- Installation von Applikationen
- Verwaltungsdienste

Implementierter Prototyp

- Issuer, Plattform Manager & MNO = eine Instanz
- Verwaltungseinheit am Telefon mit J2ME realisiert
- Web-Interface für Applikationsverwaltung

Anwendungen

- Zustellen von Karten
- Aufladen von Geld (Geldkarte)
- Tickets via SMS an das Telefon
- Coupons im sicheren Element
- Upload von Servlets in SCWS

Ausblick

- Neue Generation von SIM Karten für NFC Telefone
  - NFC (kontaktlos)
  - Webserver on Card (SCWS)
  - DRM
- Global Platform Extensions für OTA Management
  - Mobile & Remote Configuration Profil
- Trusted 3rd Parties zur Verwaltung

Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Happy to answer any questions

Gerald Madlmayr

Gerald.madlmayr@fh-hagenberg.at

www.nfc-research.at