

Mobile Transaktionen

Christian Kantner

13.10.2011



Mobile Transaktionen

- Mobiles elektronisches Gerät
 - Display + Eingabemöglichkeit
 - Internetzugang – Always On
 - SIM Karte
- Mobile Transaktionen
 - Ticketing (Bahn, Event,...)
 - Bezahlen, Überweisen
 - ID



Verbindung zur Umgebung

- Anwesenheit vor Ort muss festgestellt werden
- Eindeutige und einfache Interaktion zwischen mobilem Endgerät und lokaler Umgebung
- Bestehende technische Varianten
 - Bluetooth, WiFi
 - Barcode
 - Ortung



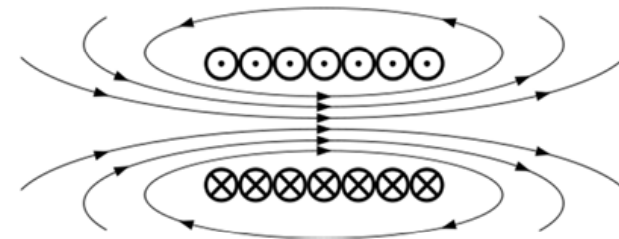
Absicherung von Transaktionen

- SIM Karte
 - Unterstützung des Mobilfunkbetreibers nötig
- Username + PW
 - Vertrauen in das OS
- Proprietäre Sicherheit
 - IOS
 - Blackberry
- Risk Management in Backend Systemen

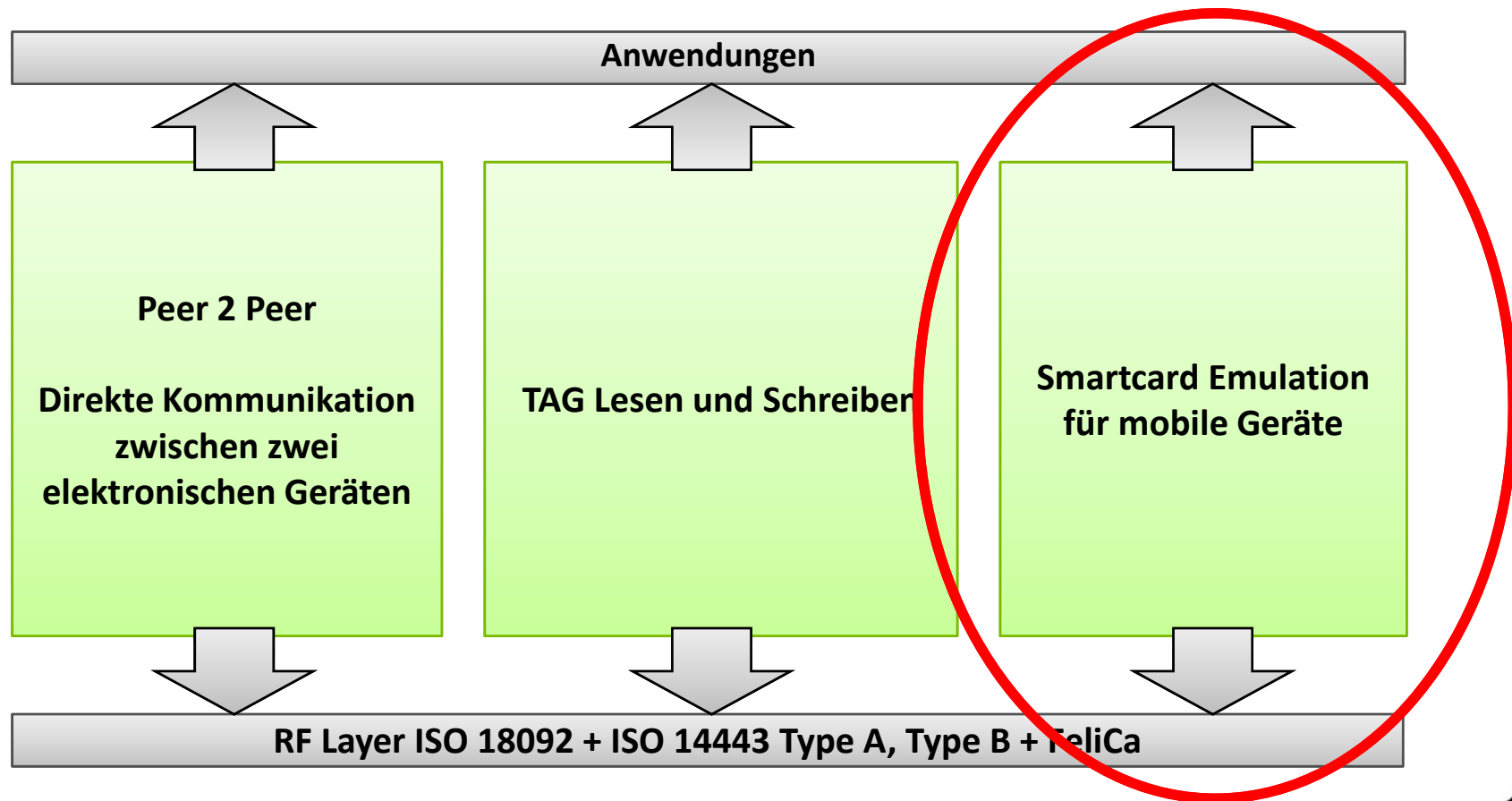
	SW only	SW + HW	Tamper Proof
Username Password	✓		
ARM TrustZone	✓	✓	
Smartcard	✓	✓	✓

NFC – Near Field Communication

- Wurzeln in bewährter RFID 13,56 MHz – Technik
- Magnetische Kopplung
- Reichweite 1-10cm
- Rückwärtskompatibel zu ISO 14443 und Smartcards
- Äusserst einfach zu benutzen
 - Kommunikation startet durch eine simple Berührung

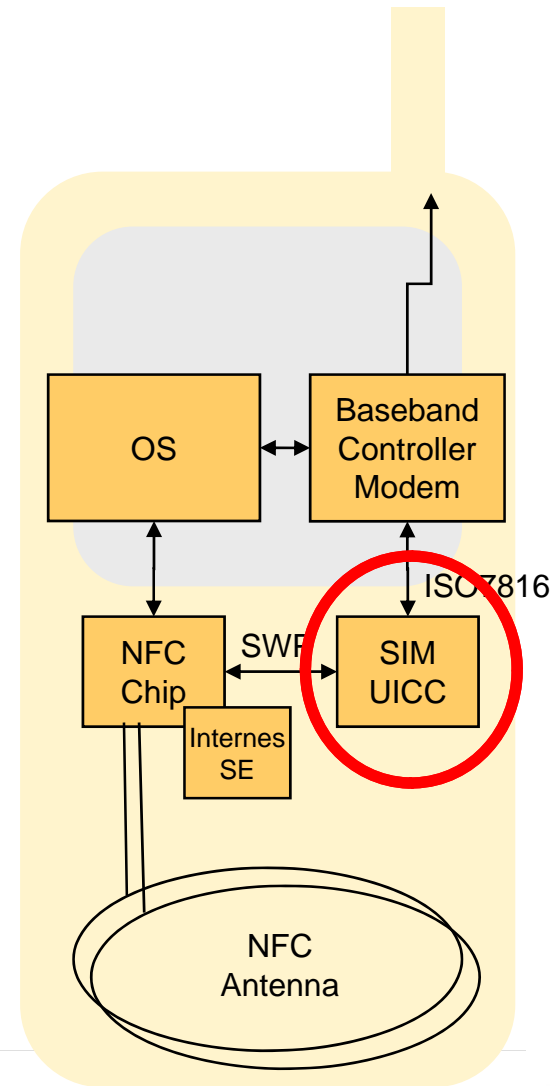
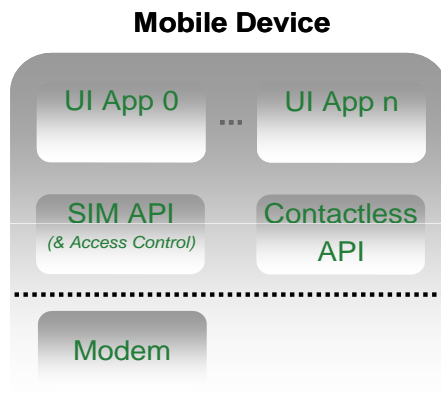
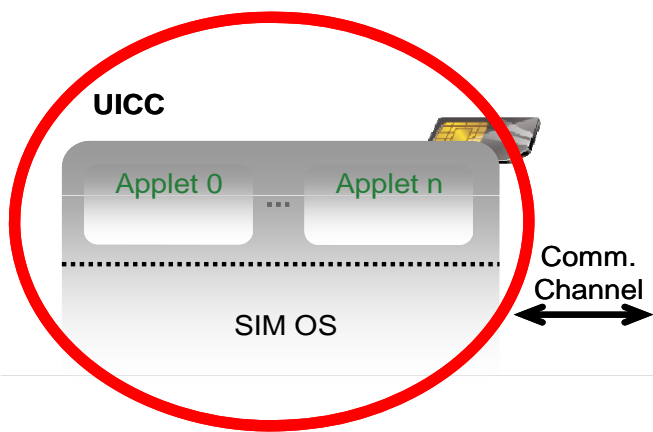


NFC - Betriebsmodi



Smartcard Emulation

- SE = Secure Element
 - Smartcard Chip
 - Javacard OS
 - Global Platform
- SIM Karte übernimmt Rolle des SE

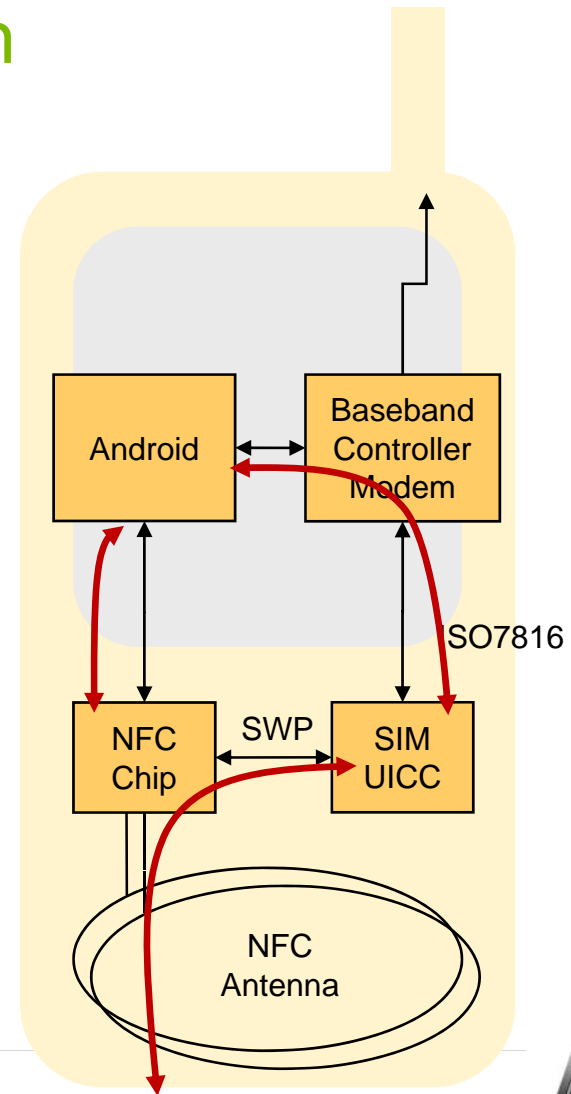


Smartcard Emulation in Aktion

NFC Transaktion startet....

NFC Chip triggered OS (zB Android)

Android App holt sich
Transaktionsdaten via Baseband und
ISO 7816 Interface von der SIM

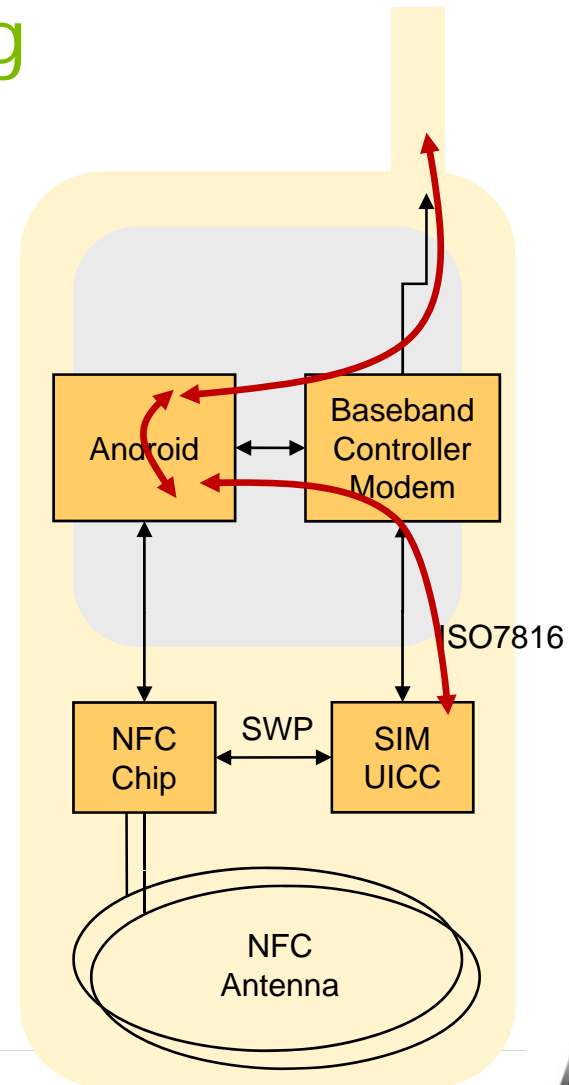


Over The Air (OTA) Verwaltung

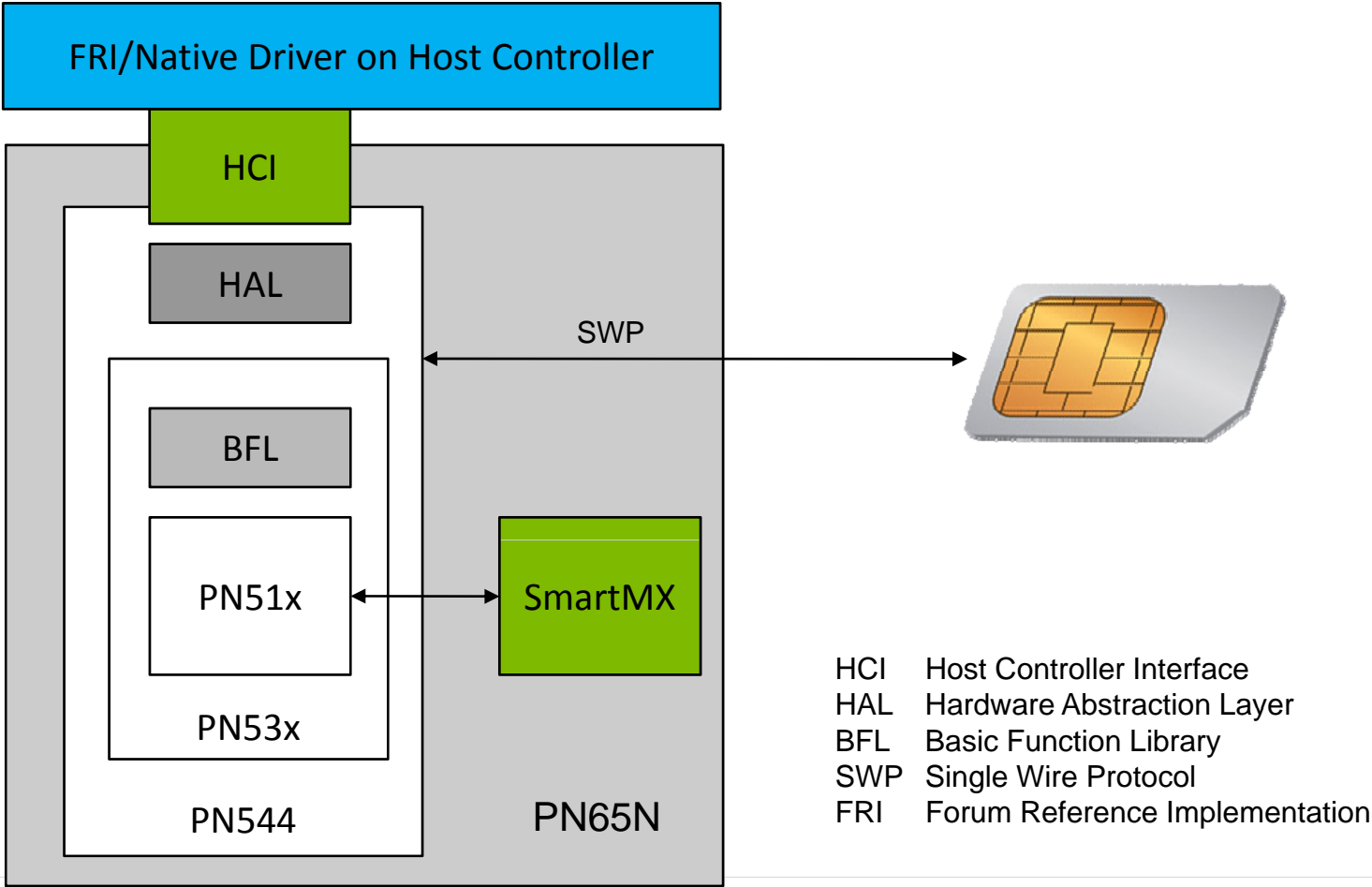
Backend triggered Android App

Android App verknüpft Backend mit der SIM Karte

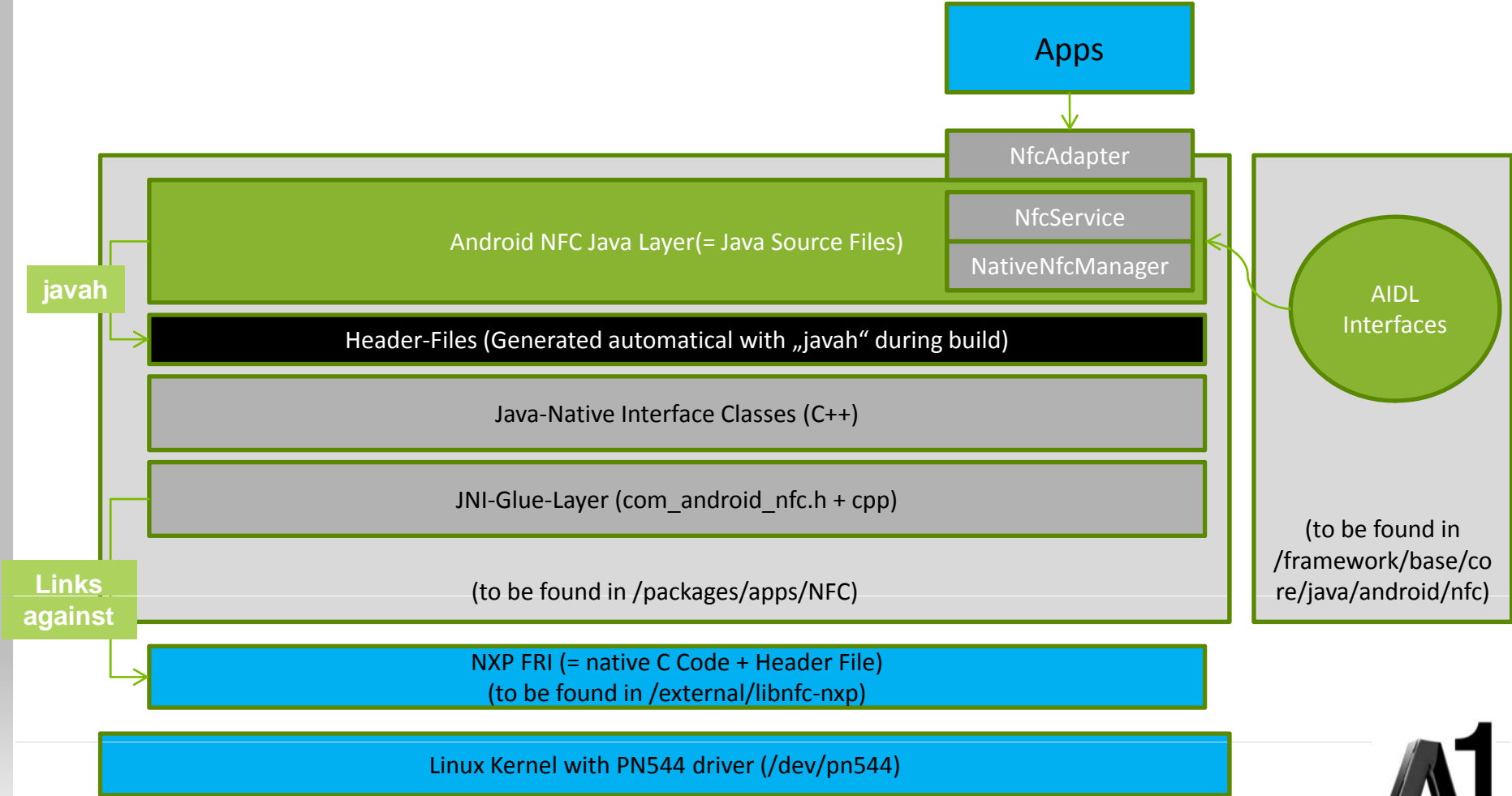
Backend spricht mit SIM, end2end Security ist sichergestellt



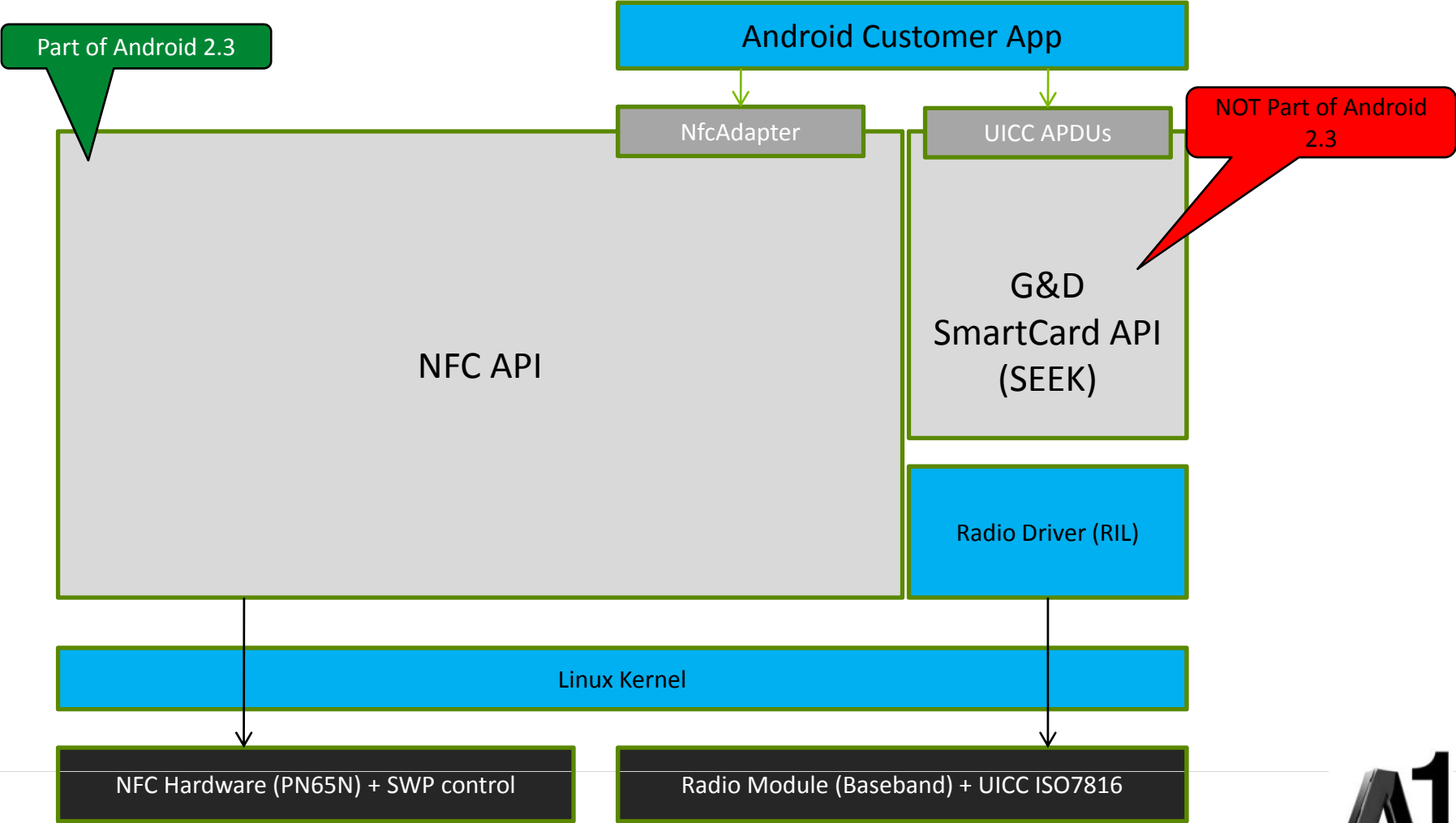
Beispiel: NXP NFC Architektur



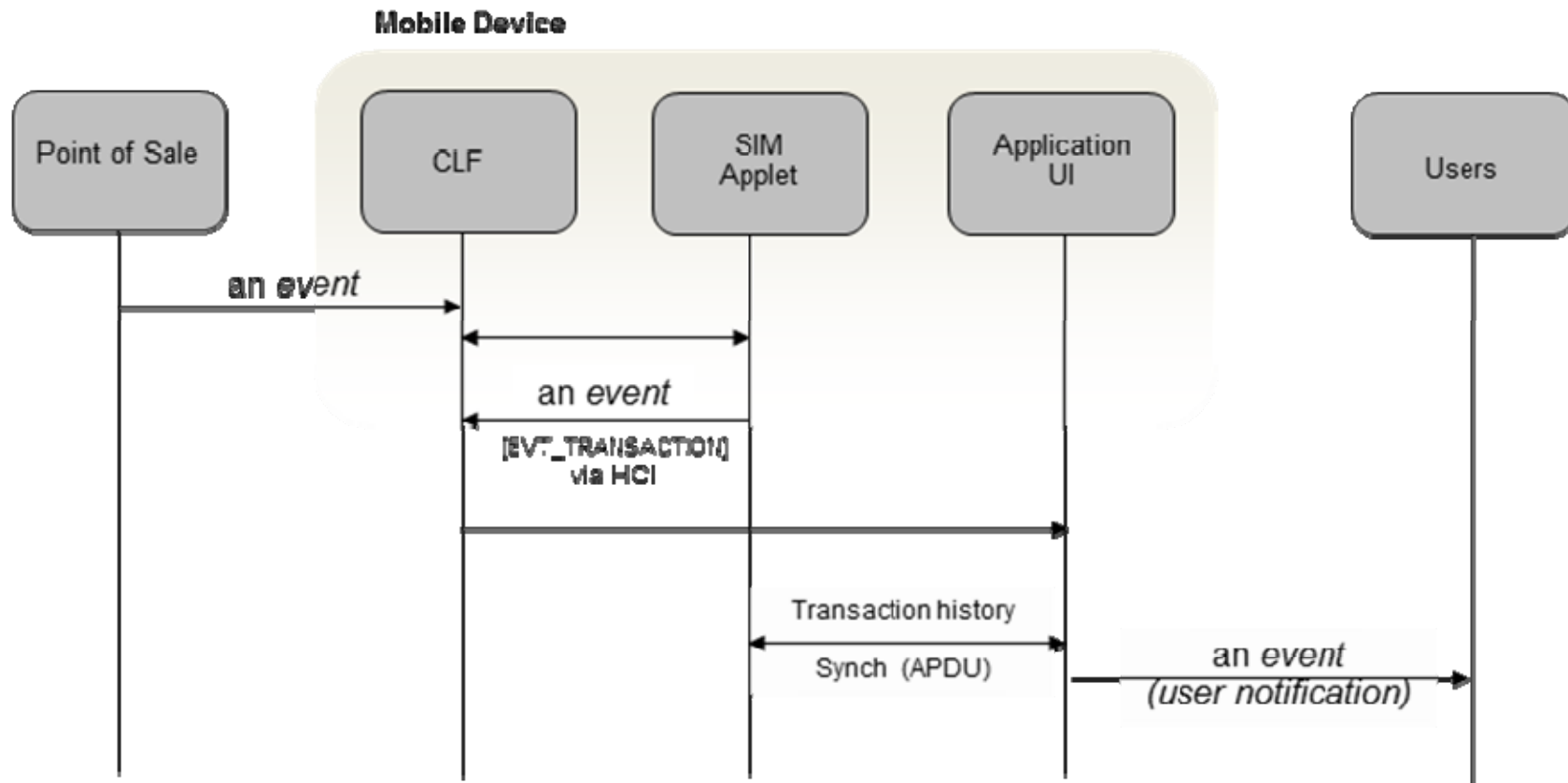
NFC und Android



NFC Android - Work in Progress



NFC POS example

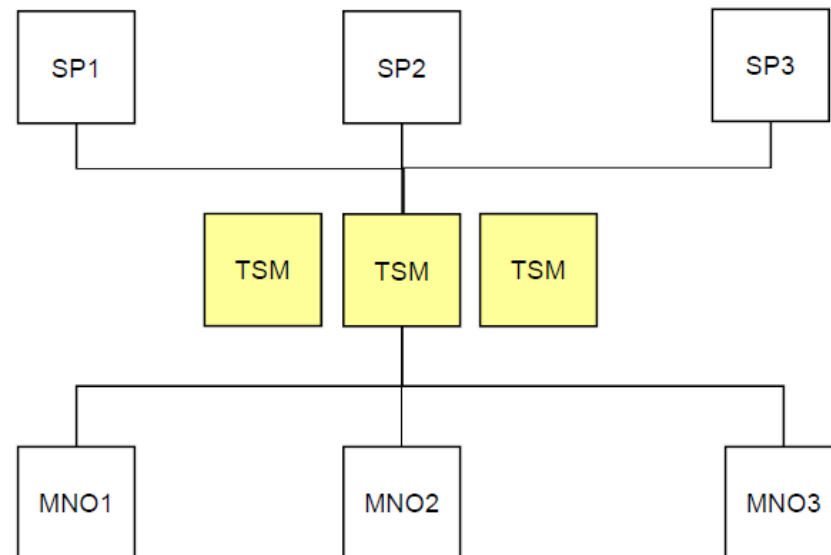


CLF Contactless Frontend = NFC Chip

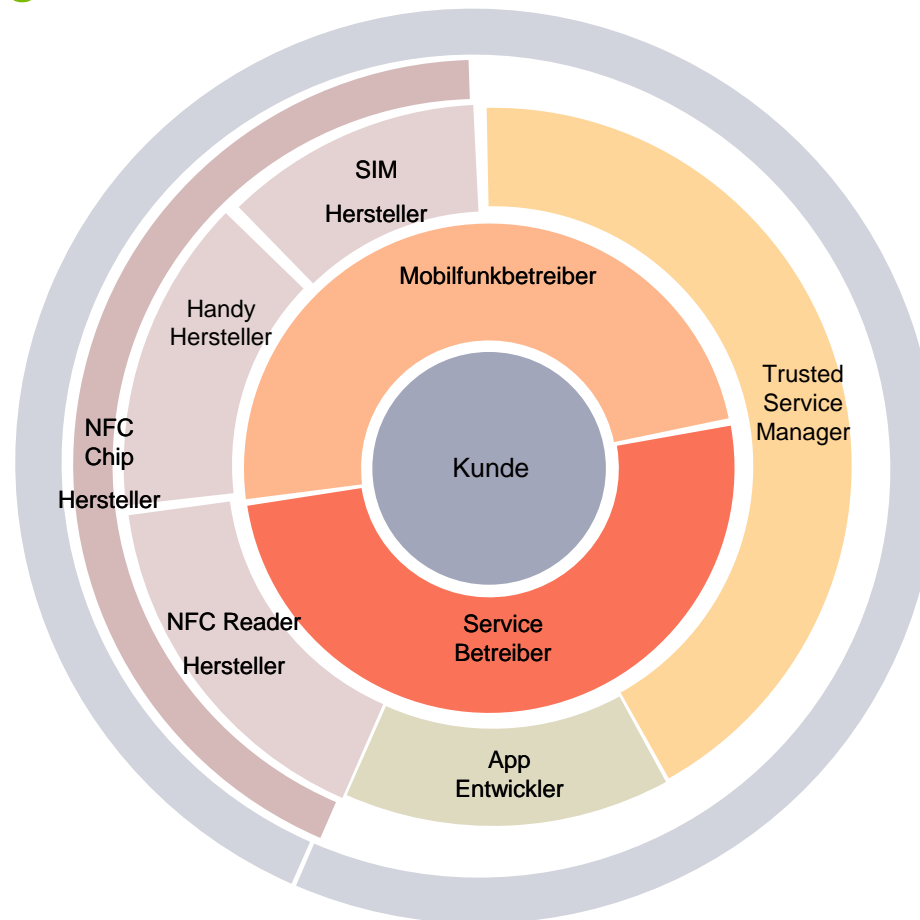


Neue Rolle – Trusted Service Manager

- TSM verwaltet die Schlüssel und Berechtigungen einer Security Domain des SE
- Service Provider können ihre Applikationen via TSM auf das SE (SIM) aufbringen



Neues Ökosystem



Auszug der Standardisierungs Gremien

- ETSI/SCP (Smart Card Platform) – SIM Karte



- EMVCo – EMV Payment, Standards für Bezahlkarten mit Chip
- GSM Association



- Mobey Forum – Financial Services



- AFSCM – franz. Spezifikationen für Mobile Contactless

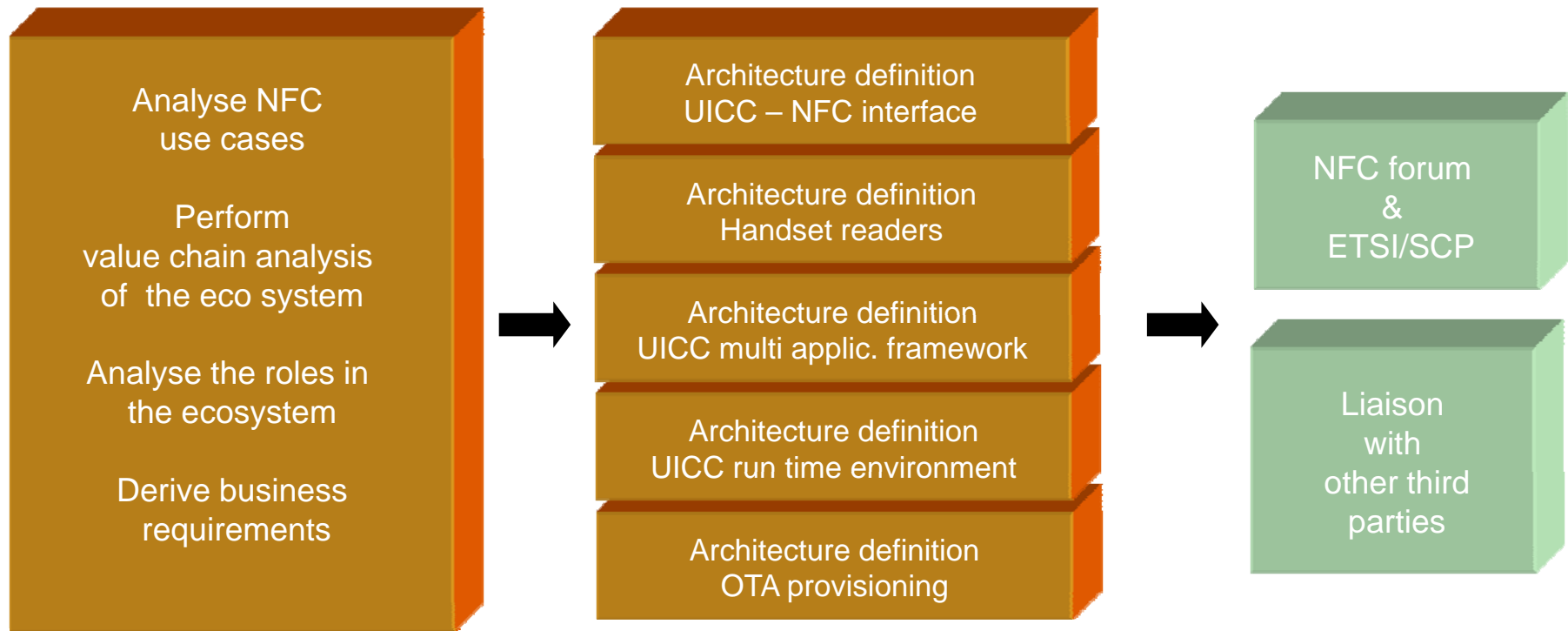
- Global Platform: Verwaltung von Java Card SE



- NFC Forum



GSMA mobile NFC Initiative



Ecosystem white paper

Technical guidelines white paper

Liaisons statements



Status NFC

- Handys mit NFC-SWP Unterstützung im Anmarsch
 - Samsung Android + Bada
 - LG, SonyEricsson
 - Blackberry
 - Nokia
 - ...
- Mobilfunk Chiphersteller integrieren NFC
- SWP SIM Karten verfügbar
- Div Zertifizierungen noch im Laufen



Zusammenfassung

- Kontaktlos ist weltweit auf dem Vormarsch
- Mit NFC entsteht eine sichere & standardisierte Infrastruktur für mobile kontaktlose Transaktionen
- Basis für neue Ökosysteme wird gelegt



Danke!

Dipl.Ing. Christian Kantner
A1 Telekom Austria
Email: christian.kantner@a1telekom.at

