Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Managing an NFC Ecosystem

Gerald Madlmayr

NFC Research Lab, Hagenberg

ICMB 2008, Barcelona

www.nfc-research.at

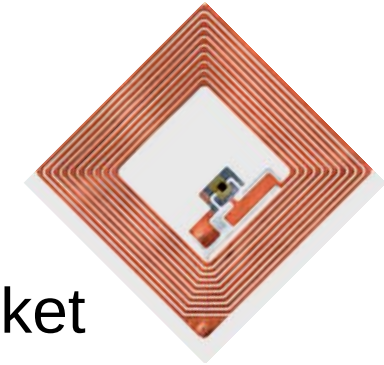
mobilkom austria

OMNIKEY

NXP founded by Philips

TU WIEN

NFC - What is it all about …



- RFID Derivate 13,56 Mhz
- Integrated in mobile devices for consumer market
- Operating Modes
  - Tag/SmartCard Emulation (PICC)
  - Reader/Writer (PCD)
  - Peer (NFC)

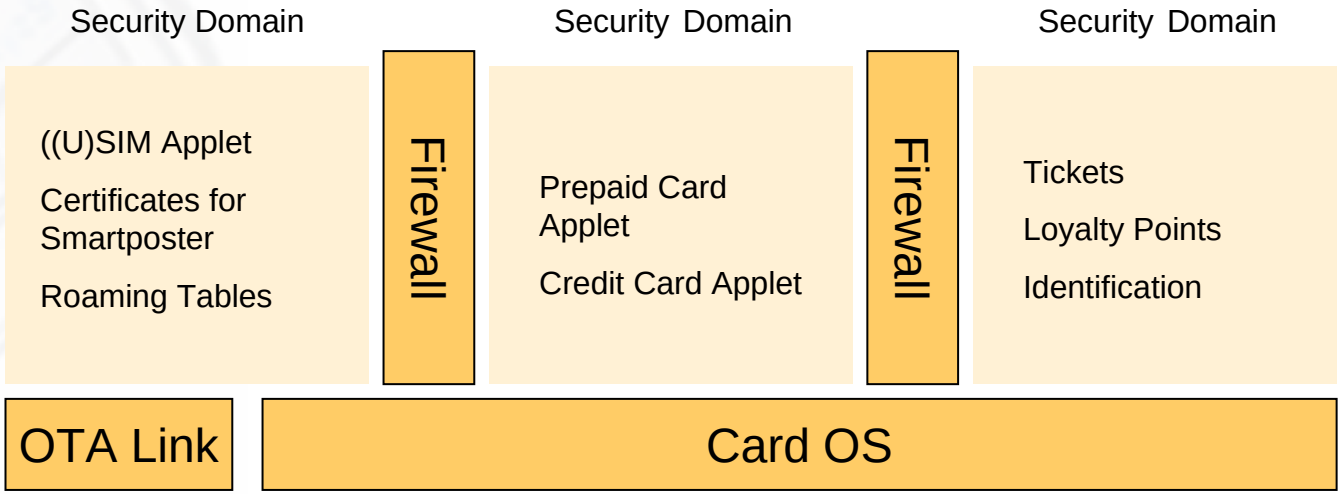
- Range: 0 – 10 cm (proximity Technology)
- Simplicity

NFC Device *Operating Modes*

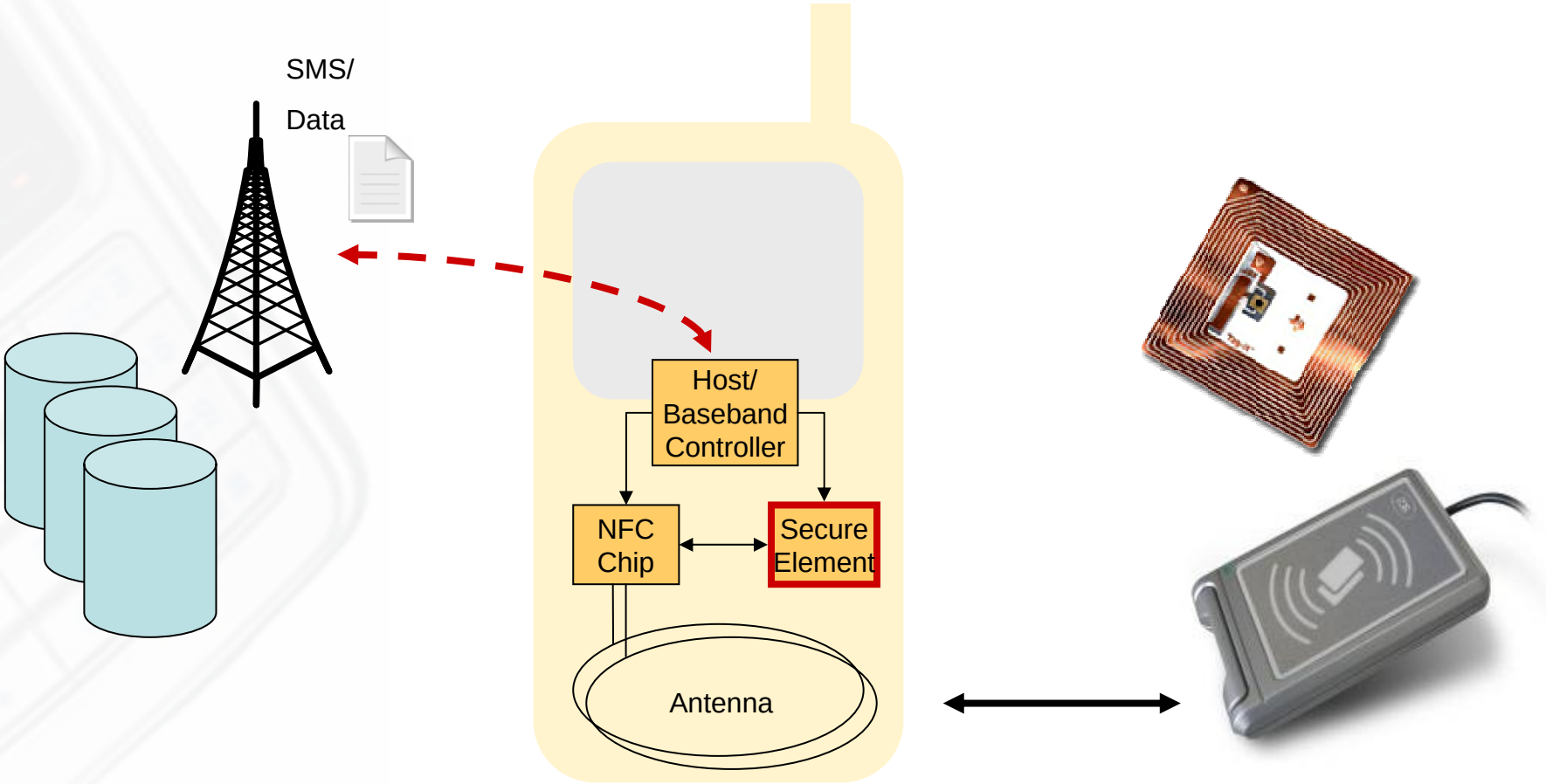
- Data exchange (P2P – NFC peer-to-peer)
  - Bidirectional connection to exchange data between devices (ISO18092)
  - WiFi, BT, P2P Payment, Contacts, vCards, …
- Reader/Writer mode (PCD – Proximity Coupling Device)
  - Mobile Device is able to read external tags/smartcards (ISO14443)
  - SmartPoster, WiFi Config, Ring-Tones, …
- Tag emulation (PICC – Proximity Card)
  - Reader can't distinguish between smartcard & tag emulation
  - Handset could contain multiple smartcards (smartcard chips)

Smartcard Emulation

- Smartcard Application is “only” software
- Upload Smartcard Applications over the air (remote)
  - Less “physical” Smartcards issued
  - Handset offers Display, Keyboard, Network to Smartcard
  - Handset substituted multiply smartcards:



Over-the-air (OTA) Services for NFC



Secure Element Implementations

Software/Application Processor

- Not tamper proofed data container
- Low implementation Costs
- Dependence on OS of Handset
- Implementation up to Service Provider
- Problem when Handset is changed

Integrated (fixed) Secure Element

- tamper proofed data container
- Extra Hardware costs
- Independence on OS of Handset
- Integration up to Handset Manufacturer
- Problem when Handset is changed

Removable Secure Element

- tamper proofed data container
- Extra Hardware costs (Card Slot)
- Independence on OS of Handset
- Integration up to Issuer (Hand needs Slot!)
- No Problem when Handset is changed

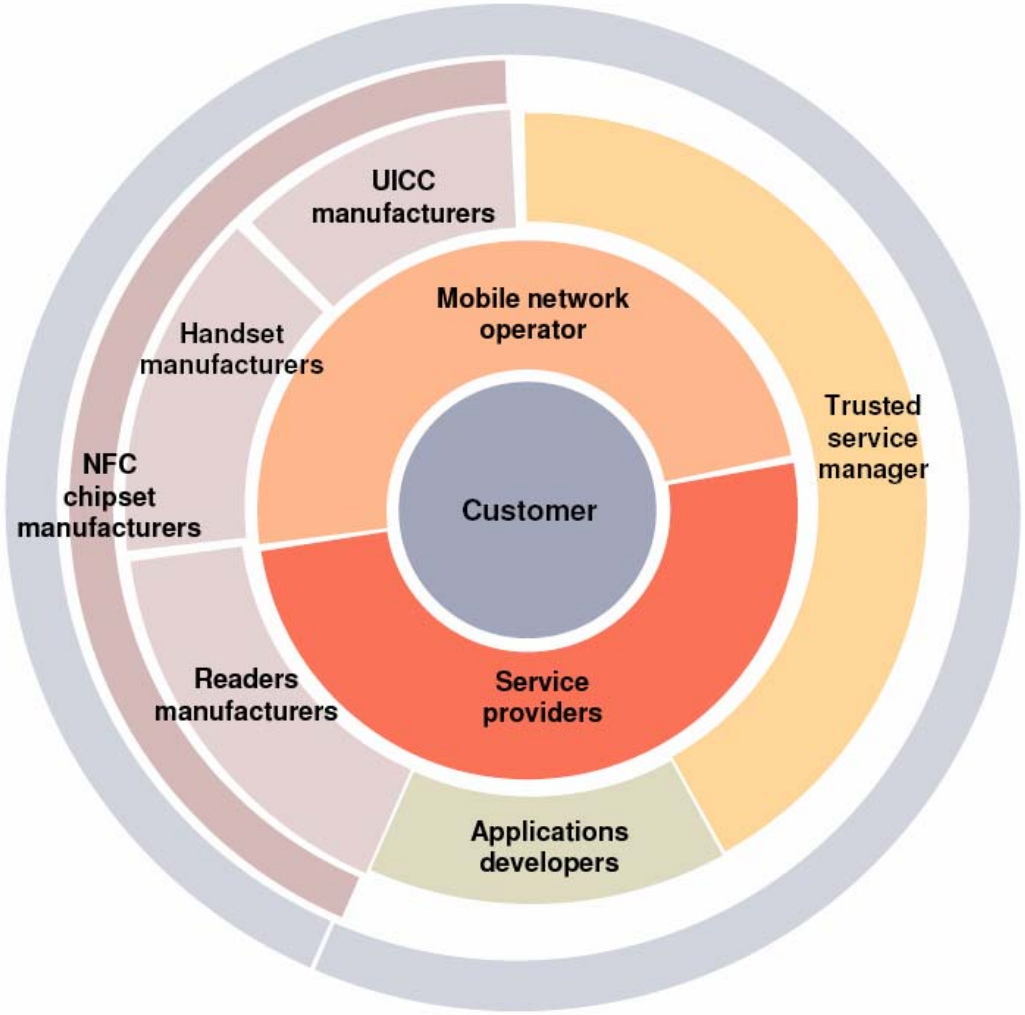
USIM

- tamper proofed data container
- No Extra Hardware costs
- Independence on OS of Handset
- Completely under control of MNO
- No Problem when Handset is changed

Management of the Secure Element

- Initialization & Pre Personalization (before issuing)
- Issuing the secure element/handset
- Personalization of Secure Element by TSM
- Installation of Applications in the Secure Element
- OTA Services (Lock, Update, …)

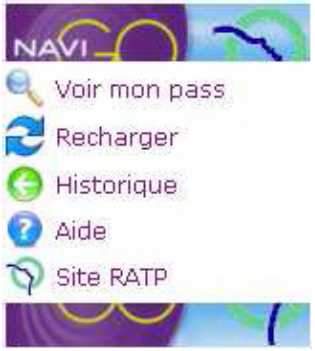
Stakeholders in an NFC Ecosystem



MNO Centric Approach

- Secure Element
  - USIM
  - Requires front up investment (Change SIMs, Backend Infrastructure)
- Issues
  - Relationship between MNO and Services Providers (eg. Banks not too good) => Ecosystem without big Service providers will not work out
  - Trust in MNO Infrastructure by Service Providers
- Pros
  - Handset (can be changed easily; everything on SIM)
  - MNO = Service Provider (MNO also offers payment, ticketing ..)

Handset Manufacturer Centric Approach



- Secure Element
  - integrated into handset
  - BOM increased
- Issues
  - Changing the Handset => move applications
  - Handset Manufacturer has not (yet) contract with user for billing purpose
  - OTA Transactions => requires MNO (also to sell handset)
  - SIM Technology gets more sophisticated => more Apps on SIM
- Pros
  - Handset Manufacturer also offer services (eg. Ovi)
  - Handset Brand important for user (eg. iPhone)

Service Provider Centric Approach

- Secure Element
  - Removable (SD-Card)
  - own handset (+ Service Provider as VMNO)
- Issues
  - Each service Provider an MNO?
  - Management of removable secure elements poses secure issues
  - Will not lease space to competitors
- Pros
  - Services Providers powerful (eg. Mastercard)
  - Services Providers want to their brand to be visible

Neutral TSM

- SE Implementation
  - Any, but Management waived to independent TSM
  - MNO/SIM Features needed for OTA Transactions
- Issues
  - Neutrality (Who is neutral?)
  - TSM knows “everything”
  - Additional Player (costly)
- But
  - Good Solution for MNO and Services Providers
  - Roll of Handset manufacturer unclear

No solutions for all markets:

- Europe
  - Chicken-Egg Problem
  - Lots of different players in each country
  - But: France has already an NFC consortia (MNOs, PTOs, Banks, …)
- US/Asia
  - CLess Infrastructure partly established
  - Few Player for big market/lots of consumers
- Japan
  - DoCoMo dominated CLess market as MNO and Services Provider
  - No 3rd party services possible (eco system “closed”)

Conclusion

- Ecosystem depends on
  - Secure Element Implementation
  - Market Situation
  - Will only work if MNO, Service Providers and Handset manufacturers work together (like France, but interntl')
- Business Model
  - Lease Space in Secure Element
  - Offer OTA Management Services
- Certification of Issuing not possible (to many players)
  - New Methods/Agreements needed

Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Happy to answer any questions

Gerald Madlmayr

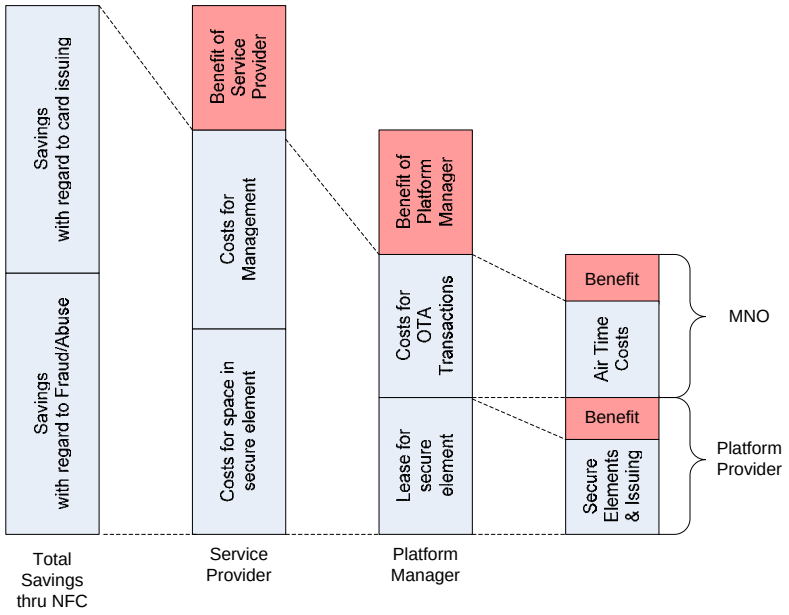
Gerald.madlmayr@fh-hagenberg.at

www.nfc-research.at

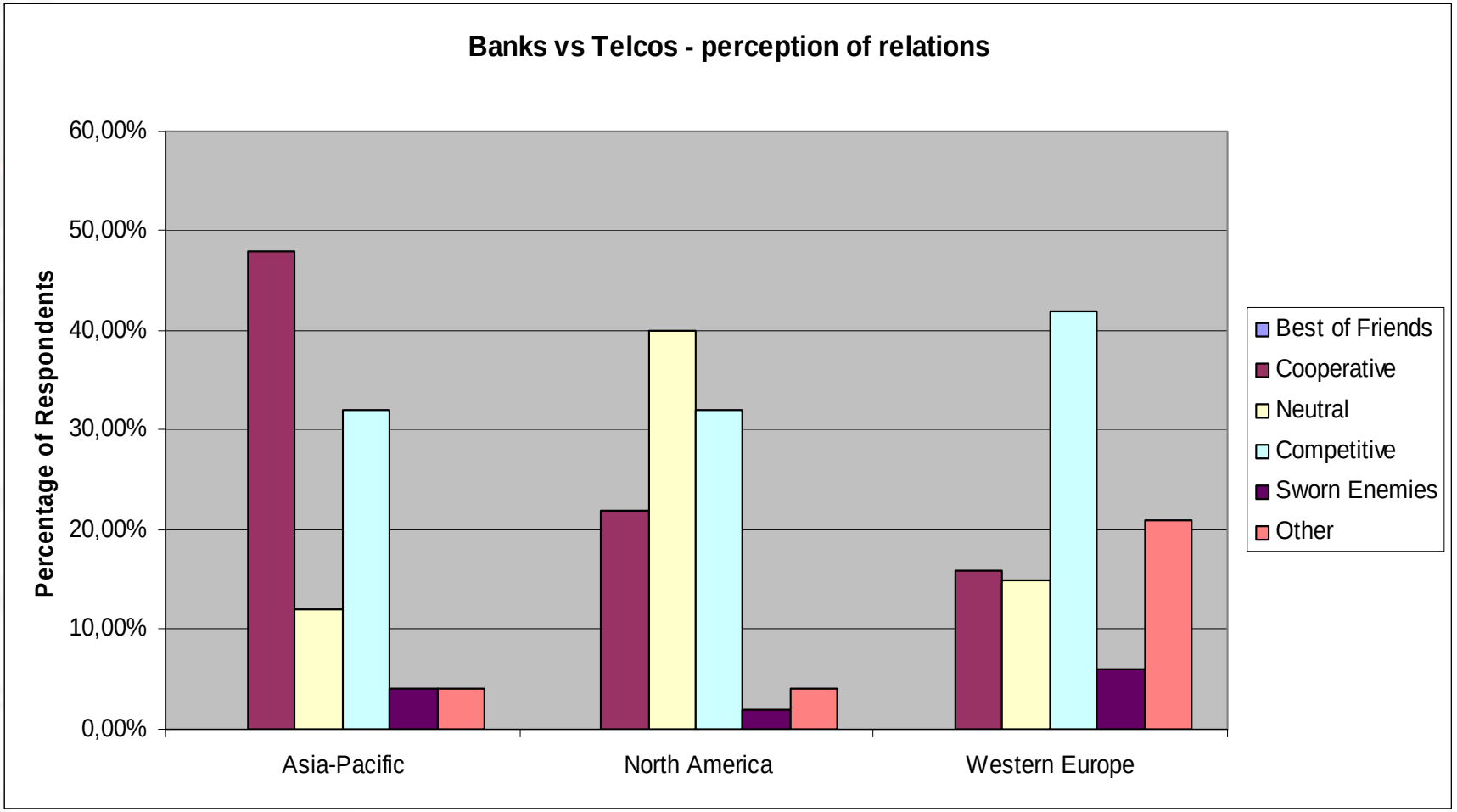
mobilkom austria · OMNIKEY · NXP founded by Philips · TU WIEN

Win-Situation for every player

- TSM act as independent player
- Involvement of Handset Manufacturer unclear
- Share Savings achieved thru NFC

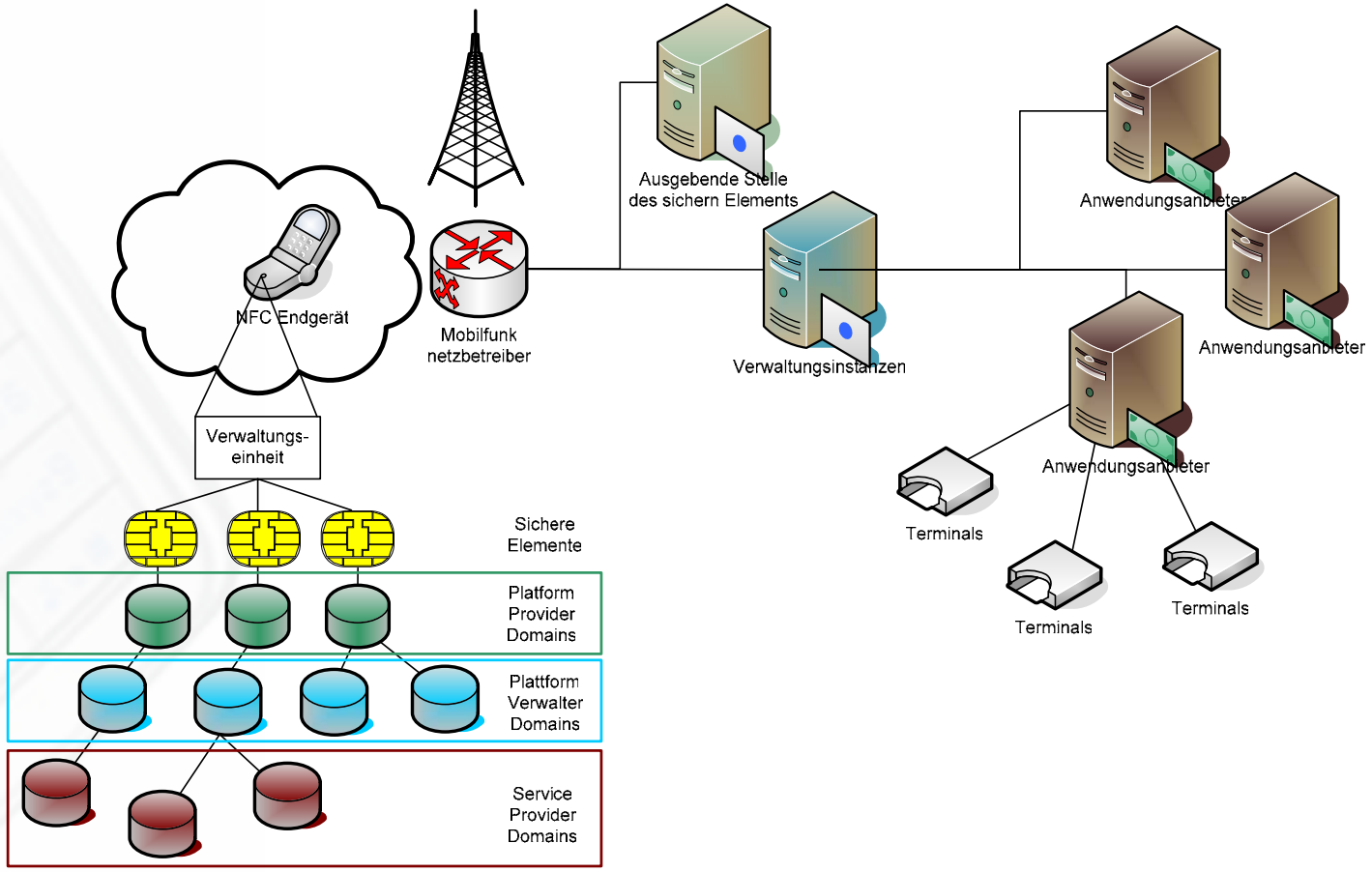


Banks vs. Telecos – Perception of Relations



Source: Edgar Dunn/IN-CLUB Survey September 2006

Technical Eco System



NFC Device Architecture