Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

The benefit of using SIM application toolkit in the context of NFC applications

Gerald Madlmayr

NFC Research Lab Hagenberg

ICMB - July 11th, 2007

Introduction

- Research Consortium
  - NXP Semiconductors Austria (formerly know as Philips)
  - Mobilkom Austria (part of vodafone group)
  - OmniKey (part of Assa Abloy)
  - University of Applied Sciences of Upper Austria, Hagenberg

- Mission
  - Analyses of technical integration of NFC along value chain
  - Goal: usable, reliable and secure NFC services for end consumer

Introduction

- Member of the NFC Forum
- Trial up and running at Campus
  - 100 participants
  - Payment Solution (Cafeteria, Vending machines)
  - Access (Labs, Offices, Garage)
  - Ecosystem/Infrastructure to test
    - Acceptance of Services
    - Usability of Services
    - New devices

Near Field Communication

- Coop between Philips/NXP & Sony
- Contactless proximity Technology
- Bases on RFID (13,56 Mhz)
- Compatible to ISO14443 (Mifare, Felica)
- Operation Modes
  - Tag Emulation (PICC): eg. Phone is access token
  - Reader/Writer (PCD): eg. Phone can read RFID tags
  - Peer (NFC): eg. Exchange of data between phones
- Range: 0 – 10 cm (0” – 3“)

NFC Phone in Smartcard Mode

- Creditcard (450 Mio. Cards per year*)
  - Mastercard: Paypass
  - Visa: Visa & Wave
- Public Transport (300 Mio. Cards per year*)
  - London: Oyster Card (Philips/NXP Mifare)
  - Hong Kong: Octopus (Philips/NXP Mifare)
  - Tokyo: Suica (Sony/NTT DoCoMo Felica)
- ID/Passport, Loyalty, E-/digital Signature

*Source: Gemalto

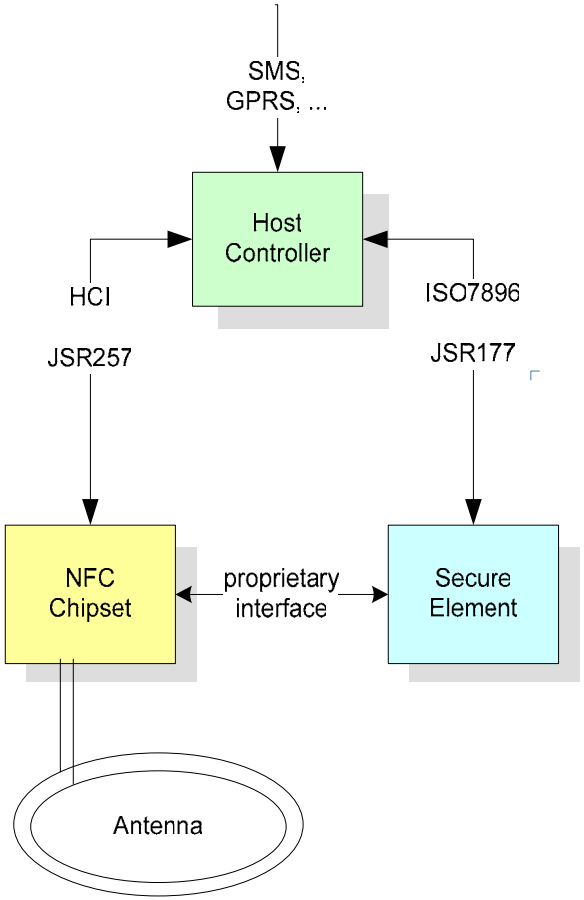
Keep in Mind …

… the application on the contactless Smartcard is only a piece of software.

Why always change/reissue the whole card, if changing the software would do?

NFC and the Secure Element (SE)

- Dynamic environment for programs and data
- SE can be accessed through
  - Host Controller (internal)
  - RF Field (external)
- NFC device/SE as a proxy for PAN-WAN communication
- Questions are
  - How to implement SE?
  - Who manages/wants to manage SE (and makes extra revenue)?



Implementation of SE

- SIM Card
  - Business of/Belongs to the Operator
  - No contribution to BOM of handset (SIM more expensive)
  - “NFC” SIMs can be used in “non-NFC” handsets
- Secure Memory Cards
  - Card belongs to consumer
  - Increase in BOM (card reader required in every phone)
- Additional Smartcard Chip (integrated in Handset)
  - Handset belongs to consumer
  - Increase in BOM (cost for smartcard chip)

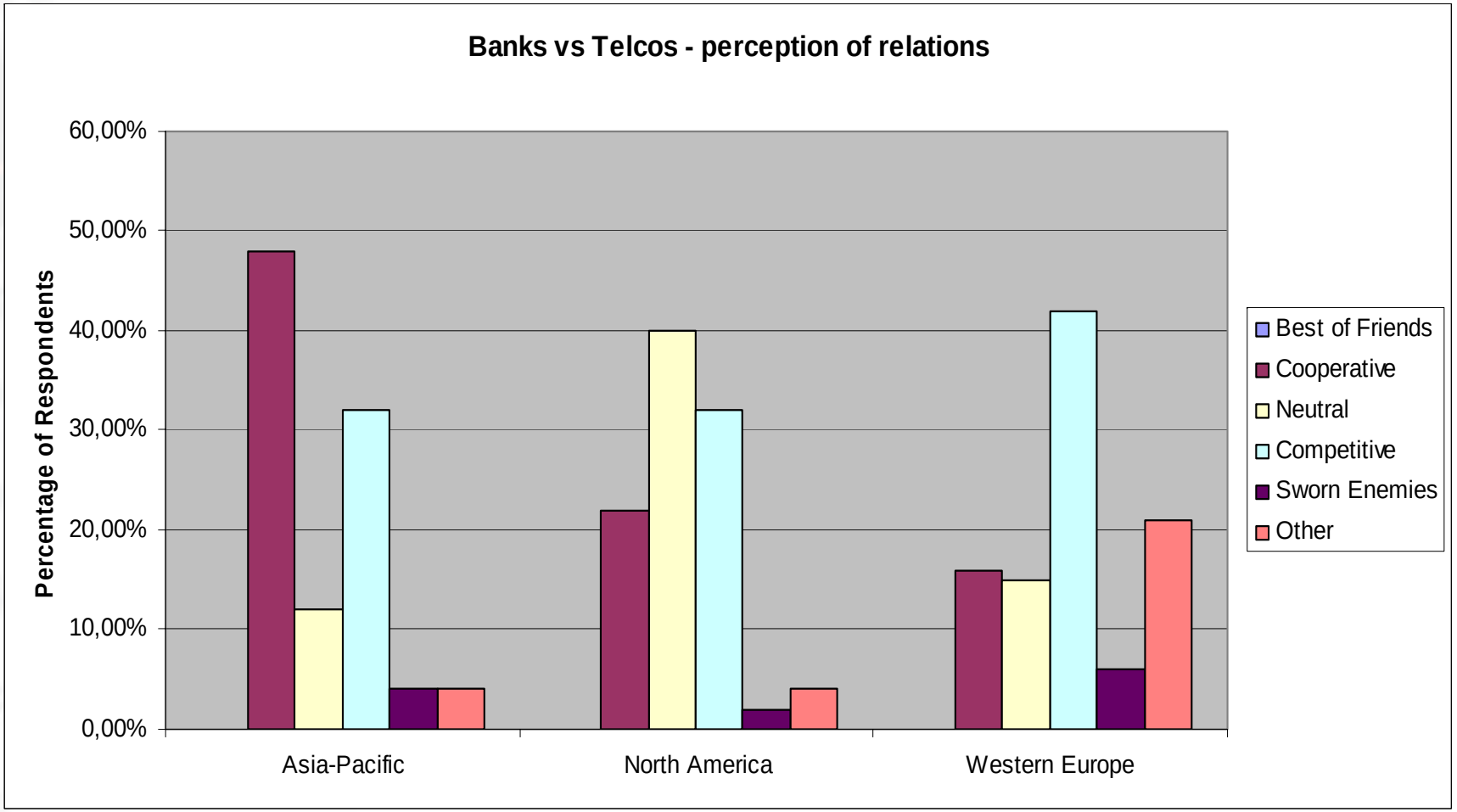
Management of SE

- Management of SE itself (“Issuer”)
  - Mobile Network Operator
  - Bank/Credit Card Company
  - Handset Manufacturer (integrated IC)
  - Trusted 3rd Party
  - Government
  - (Consumer)

- Management of Data in SE (“Application/Content provider”)
  - Instances above and …
  - (Public) Transport Operators
  - Merchants using SE as Loyaltcard
  - Event & Ticket Offices
  - … many more

Secure Element/Data/Apps must NEVER leave chain of trust!

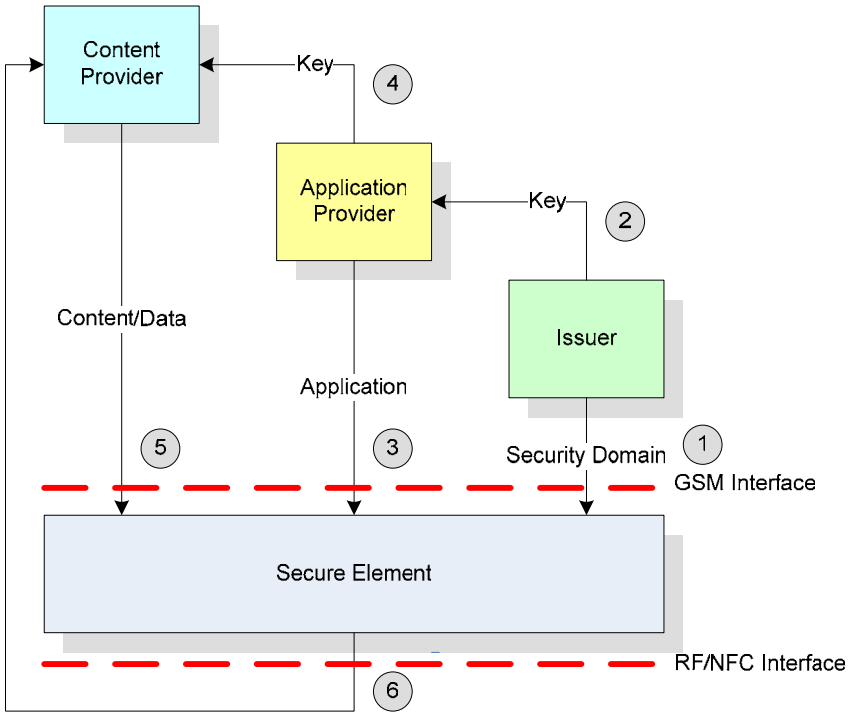
Banks vs. Telecos – Perception of Relations



Source: Edgar Dunn/IN-CLUB Survey September 2006

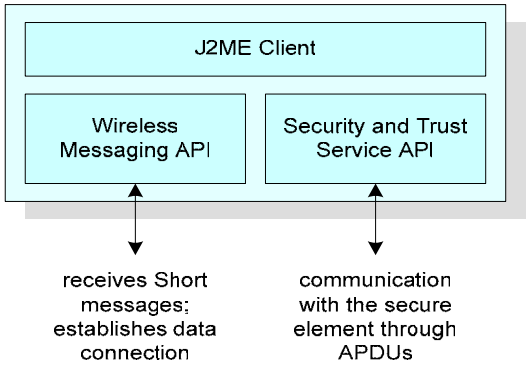
Processes in an NFC Infrastructure

1. Personalization
2. Setup of Security Domains
3. Upload of Applications OTA
4. Application Sharing
5. Upload of Content OTA
6. Download of Content over RF



Approach 1: J2ME Solution

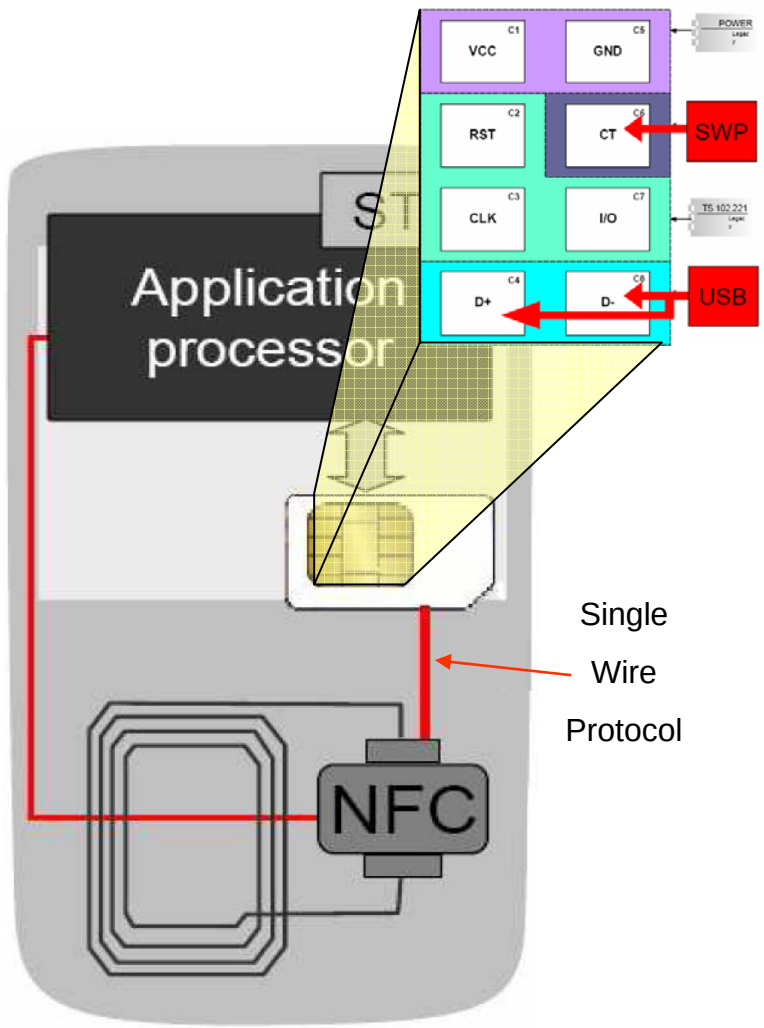
- Send SMS to handset
- J2ME Application starts & establishes a data connection
- Load data & applications into SE
- J2ME application only proxy
- Problems
  - J2ME can be removed by user
  - Process of Transaction can be stopped by user
  - J2ME Platform differs from phone to phone



The SIM as the SE

- GSMA specifies protocol/interface for the SIM to be used with NFC Chips: SWP (Single Wire Protocol)
- SIM Card is the cheapest solutions for the SE in regard to BOM
- SIM Card is less often changed than handset
- SIM Card is upgraded in value
- => SIM Card is likely to be the SE for future Handsets

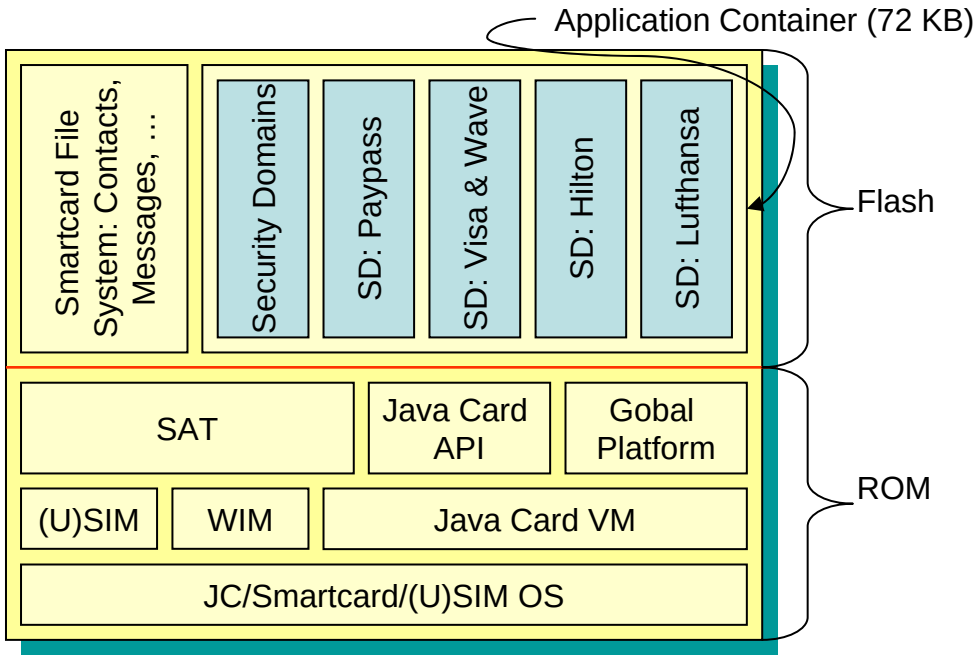
This does not exclude other parties than the MNO to manage the SE, but MNO is likely to be the manager of the SIM/SE

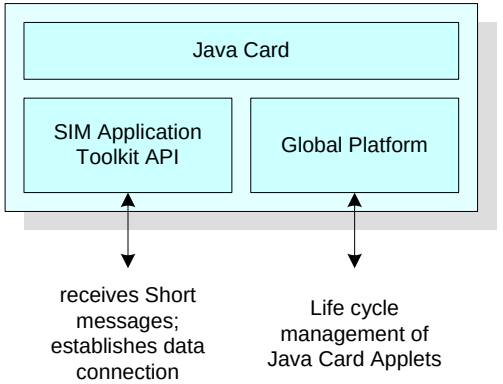


Source: Images by TIM, Gemalto

Approach 2: SAT

- SIM Card = Smartcard with Java Card OS
- SAT is also an extension for Java Card
- Can make use of data bearers of the handset (SMS, GSM, GPRS, BT, IrDA …)
- Management Application already integrated in SE
- BIP (Bearer independent protocol) needs to be defined





Benefits of SIM Application Toolkit

- Closed Systems – Everything runs on SIM/Secure Environment
- SIM/JCOP is Standardized Development Platform
- Exchange of handset does not effect application
- Independent from Handset Operating System
- Possibility of OTA Management of Apps (hidden to user)
- Basic operation without battery (good or bad?)
- Issues:
  - GUI not as sophisticated as in J2ME (Usability)
  - Change of the MNO causes work/trouble =>
    applications need to be moved to different SIM Card

Business Case

- Premises: SIM card = SE - Manager of SE = MNO
- Mobile Network Operator leases space to application/content providers
  => more revenue
- In case of lose or theft the SE element could be deactivated remotely
  => less cost (call centers, abuse/fraud)
- Application provider do not need to issue cards any more
  => OTA/RF distribution of “cards”/content to consumer
  => more secure/faster than sending cards/content by mail
- More Revenue due to faster transactions *
  - McDonalds: **6 seconds** saved on payment = **+ 1 %** revenues
  - Tesco: **1 second** saved on payment = **10 M£** savings/year

* Source: Gemalto

Business Case - Costs

- MNO need to operate trust centers for application management
- Bigger/New SIM Cards (need to support communication with NFC Chip and SAT)
- Process of issuing new/changing SIM Cards (every consumer needs a new SIM)
- Move data from old to new SIM (customer service)

Conlusions

- MNO leases space on the SIM
- SAT allows simple & reliable remote management of applications
- NFC intuitive and easy to use technology for proximity transactions *
- Problem: no handsets yet available for mass market
  => ABI Research: by 2010 400 Mio. Handsets;

* Source: NFC Trial Report, Hagenberg (to be published)

Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Happy to answer to any questions

Gerald Madlmayr

gerald.madlmayr@fh-hagenberg.at

+43-7236-3888 7149

www.nfc-research.at