Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Management of Multiple Secure Elements in NFC-Devices

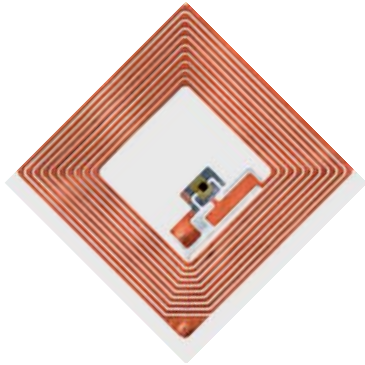
Gerald Madlmayr

NFC Research Lab, Hagenberg

Cardis 2008, Royal Holloway University of London

www.nfc-research.at

NFC – Near Field Communication



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

- Range: ~ 4 cm (proximity Technology)

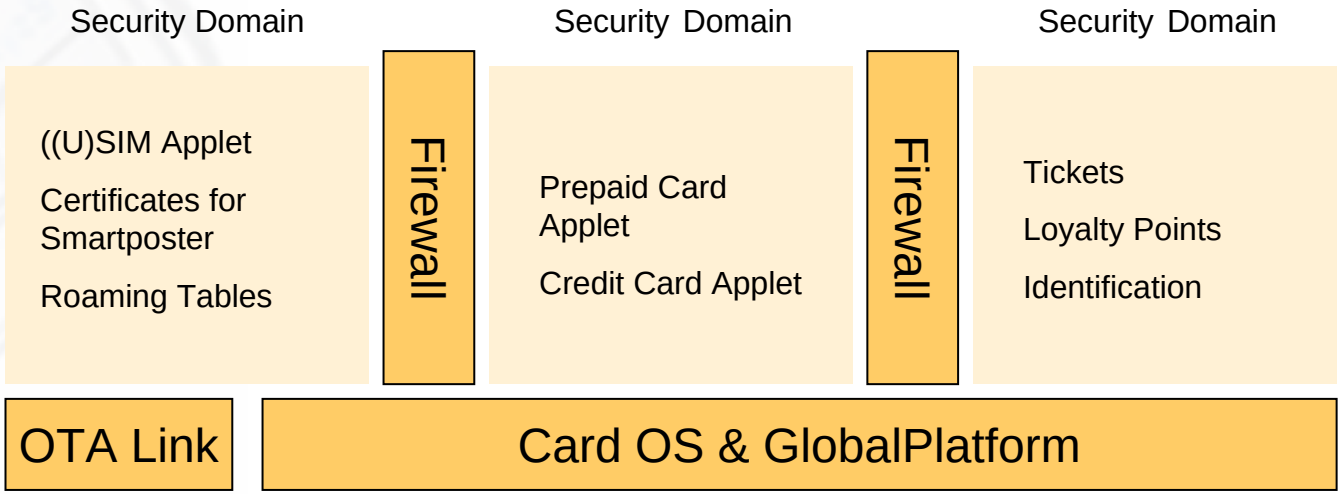
- Simplicity: Touch & Go
- Goal: Interoperability (Felica/ISO14443-A/B in one Device)

NFC Device *Operating Modes*

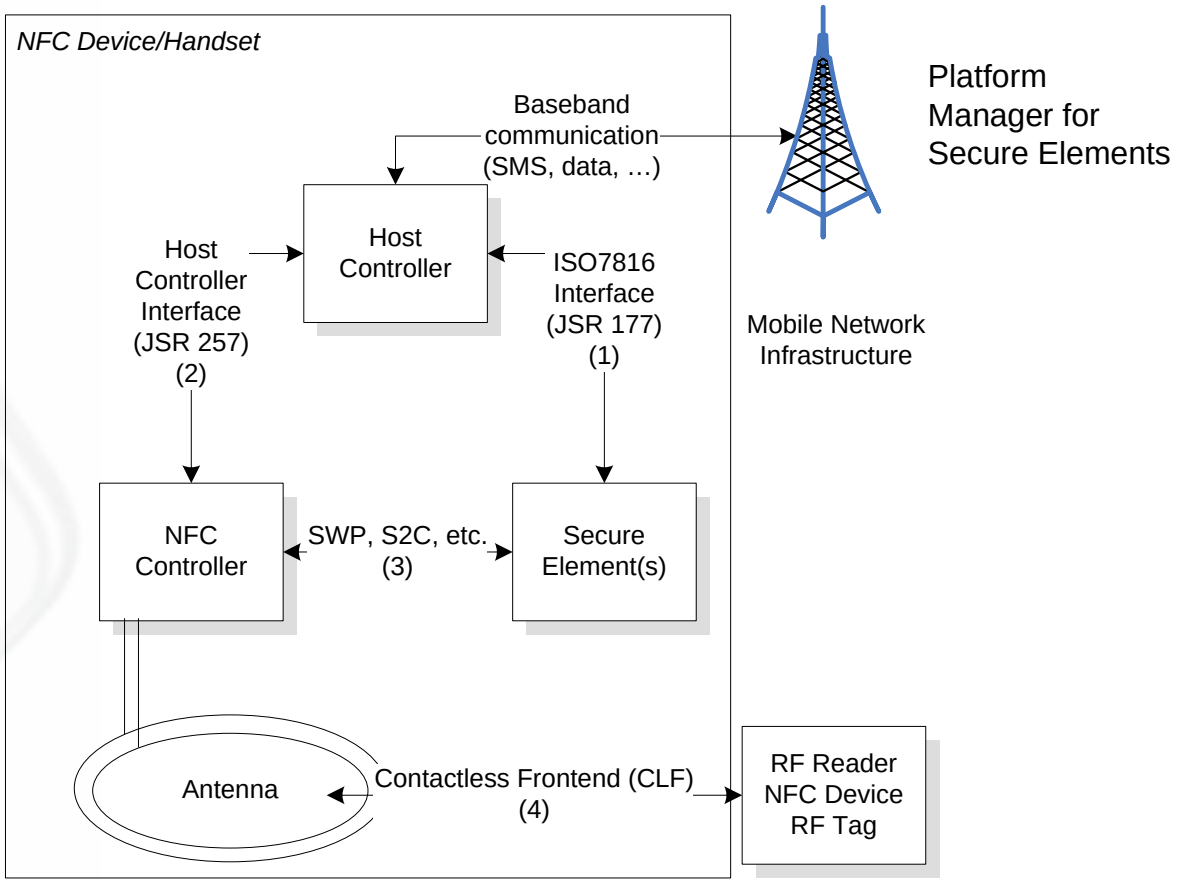
- Data exchange (P2P – NFC peer-to-peer)
  - Bidirectional connection to exchange data between devices (ISO18092)
  - WiFi, BT, P2P Payment, Contacts, vCards, …
- Reader/Writer mode (PCD – Proximity Coupling Device)
  - Mobile Device is able to read external tags/smartcards (ISO14443)
  - SmartPoster, 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 (eg. JavaCard)

- 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:



OTA-Manager for Secure Element



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

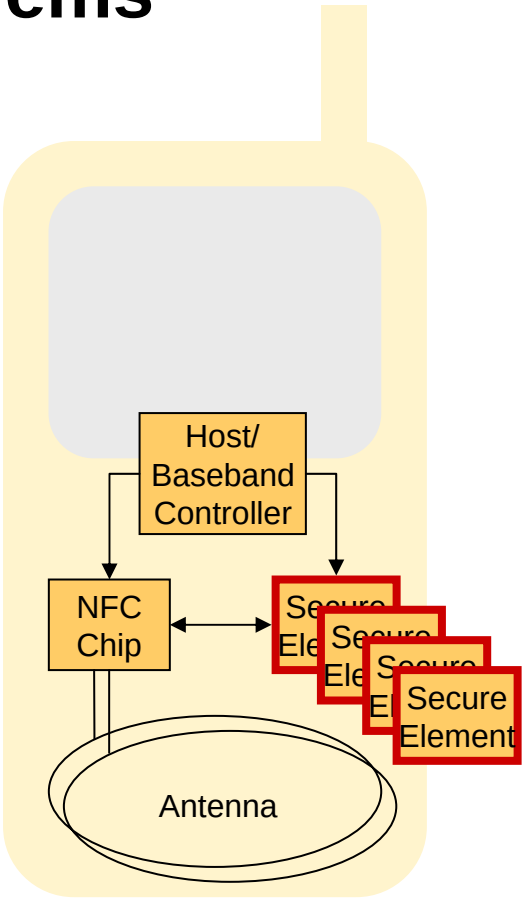
- tamper proofed data container
- Extra Hardware costs (Card Slot)
- Independence on OS of Handset
- Integration up to Issuer (phone needs Slot)
- No Problem when Handset is changed

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

Multiple Secure Elements - 2 Problems

- (1) What does an external reader “see”?
  - P2P random ID
  - One ID/Secure element
- (2) How to manage remove able secure elements?
  - OTA Management vital for Ecosystem (manager!)
  - What if secure element is put in a different device?

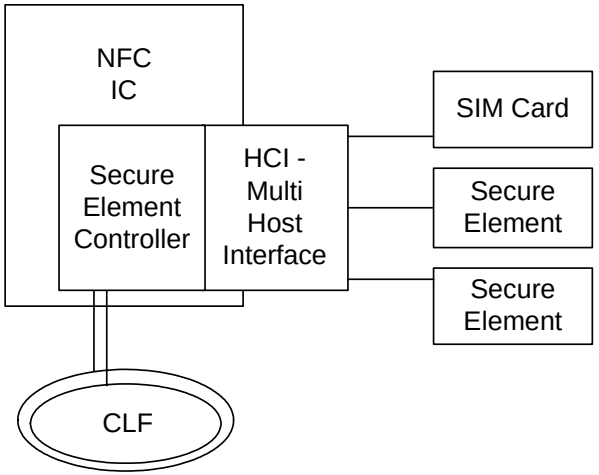


(1) What does an external reader “see”?

- Some Readers/PayPass (= CLess Creditcard) Readers do only support one Smartcard/UID in the field
  - no anti-collision implemented
- Solutions
  - Explicit Select (UICC, SecureSD, P2P …)
    - No Touch and go any more
    - Which application is on which SE?
  - Time Multiplex
    - After one SE is in ‘HALT’, present new UID
  - Aggregation and Representation by one UID

Aggregation and Representation by one UID

- Secure Element Controller (SEC) routes Data from Reader to Secure Element (SE)
  - On insert/Boot of Device, SE signs up at SEC
  - Routing according to modulation scheme (A/B/Felcia/P2P)
  - SEC keeps table of AIDs (JavaCard)
  - Minor Problem: Proprietary Cards
    - Mifare/MAD-IDs/Crypto-1
    - 1 K Classic stores 16 MAIDs (= 2 Blocks/1Sector)
    - SEC could keep “big” MAD => more Blocks
    - Felcia, other than Mode 0 (encryption)

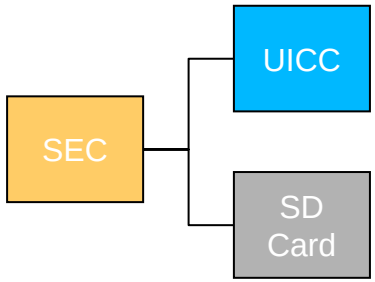


(2) How to manage remove able secure elements?

- Trusted Service Manager (TSM) associates MSISDN with the Secure element to manage.
  - What if secure element is put into new device?
  - What if secure element was stolen and put into a new device?
- Secure Element should be able to tell the TSM if device was changed
  - Activation of SE after boot of device/on insert
  - Applets can check if SE is not activated
  - Dedicated “Activation-Applet” in the Issuer Security Domain

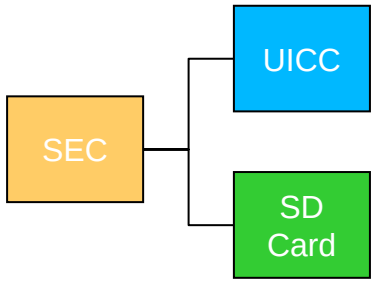
Activation of UICC

- SEC selects Activation Applet
- Asymmetric Challenge Response
- UICC can verify Certificate of SEC by OTA/BIP connection (with TSM/MNO)
- SEC advises the UICC to establish secure connection to Issuer to check certificate of UICC
- Flag in Activation Applet of UICC is set
- UICC and SEC store Certificate of each other to avoid data connections in the future



Activation of SD-Card

- SEC and UICC trust each other
- SEC selects Activation Applet of SD-Card
- Asymmetric Challenge Response
- SD Card request pipe to UICC
- Asymmetric Challenge Response
- UICC verifies Certificate of SD-Card
- SD-Card advises the UICC to establish secure connection to Issuer to check certificate of UICC/SEC.
- SD-Card verifies Certificates of UICC/SEC
- SEC verifies Certificate of SD-Card (ask UICC)
- SEC activates SD-Card



Conclusion

- When integration multiple Secure Elements into one device, backwards compatibility is not granted
  - Aggregation of SEs and only presenting one UID to the reader is a feasible solution
  - Does not require any changes to the reader infrastructure
  - Secure Element Controller (SEC) routes data streams
- Management of removable Secure Elements must be assured
  - Secure Elements need be activated before being used
  - Secure Element Controller (SEC) handles communication

Next Step: Implementation

- Use NFC Chip PN544 (first Engineer Samples available since 08/2008)
- Chip features already HCI (Host Controller Interface) and allows communication between SEs based on pipes
- Integration into NFCBox (includes NFC Chip + AVR for Program Logic)
- Use of Single Wire Protocol SIM Card & SD-Card in NFCBox
- 2nd Step: Integration into Mobile Device (Free Runner/OpenMoko)

Near Field Communication
Research Lab
Hagenberg

FH OBERÖSTERREICH
University of Applied Sciences

1st International IEEE Workshop on Contactless Security (CLessec) http://www.nfc-research.at/clessec

in Fukuoka, Japan

Happy to answer any questions

Gerald.madlmayr@fh-hagenberg.at

http://www.nfc-research.at

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