OBERÖSTERREICH

An Approach To NFC‘s Mode Switch

NFC-Research Project

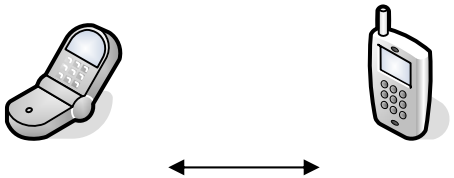
- Launch: Fall 2005
- Member of NFC Forum for Standardization
- Different Areas of Interests
  - Hardware Development
  - Use cases and Software/Application Development
  - Usability
  - Security
- NFC Trials on University Campus

NFC?

- NFC = Near Field Communication
- NFC is a wireless technology enabling data exchange within a range of up to 10 to 15 cm.
- NFC Devices have three operation modes:
  - P2P: Two devices exchange data bidirectionally with up to 424 kBit/sec.
  - Reader/Writer: A NFC device reads and writes existing RFID cards/tags (Mifare, Felica, ISO14443)
  - Card Emulation: A NFC device acts as contactless smartcard and is being recognized by existing RFID readers.

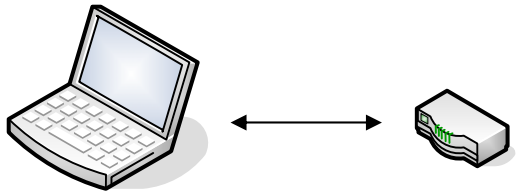
P2P Mode

- Hold two mobile phones together to exchange data.



Photos, Contacts

- Automatic setup of a WLAN link between an access point and a notebook.



Configuration data (Keys etc.)

Reader/Writer Mode

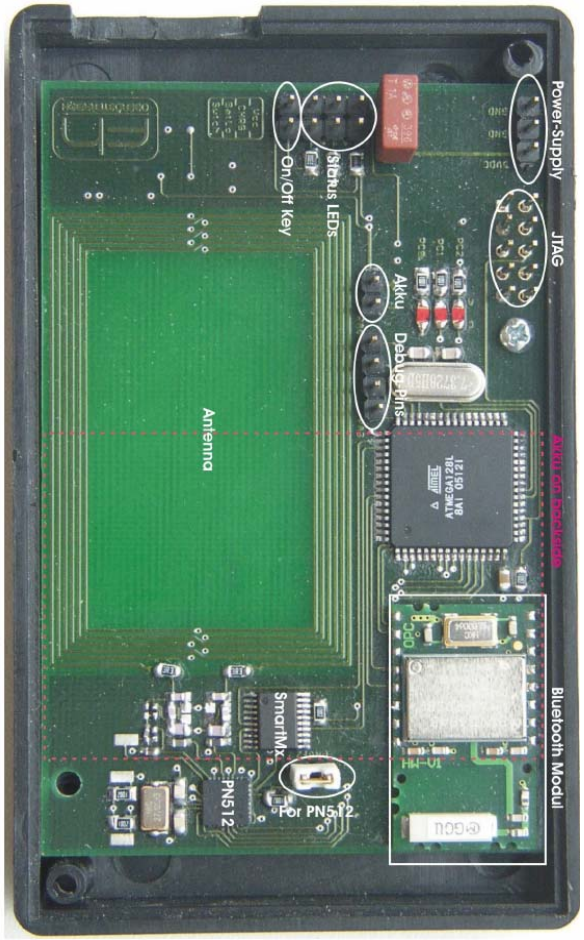
- Smartposter: On an RFID tag additional information is stored (e.g. a URI). It can be read and processed by an NFC device (e.g. URI is opened in the appliance‘s browser). This spares entering or memorizing information.

Card Emulation Mode

- The NFC device emulates a contactless smart card and can be used for access and payment solutions. Sensitive information is stored in a secure element (Secure IC).

NFC Hardware

- Analog circuits: antenna, modem
- NFC IC: PN512
  low-level protocol issues
- Microcontroller: ATmega128
  runs firmware, host-communication
- Secure Element: SmartMX
  JCOP/Mifare card, for secure transactions
- Bluetooth: serial connection to host
- Battery-powered

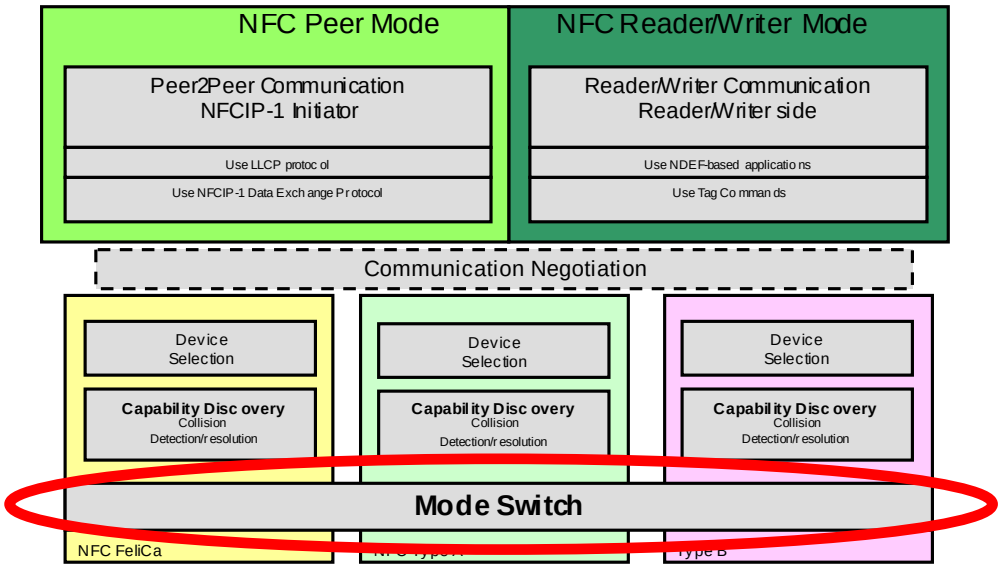


Mode Switch (1)

One of the most basic components in the protocol stack

Responsible for:

- Detection of other devices (Initiator)
- Advertising of own presence (Target)
- Device deactivation



Mode Switch (2)

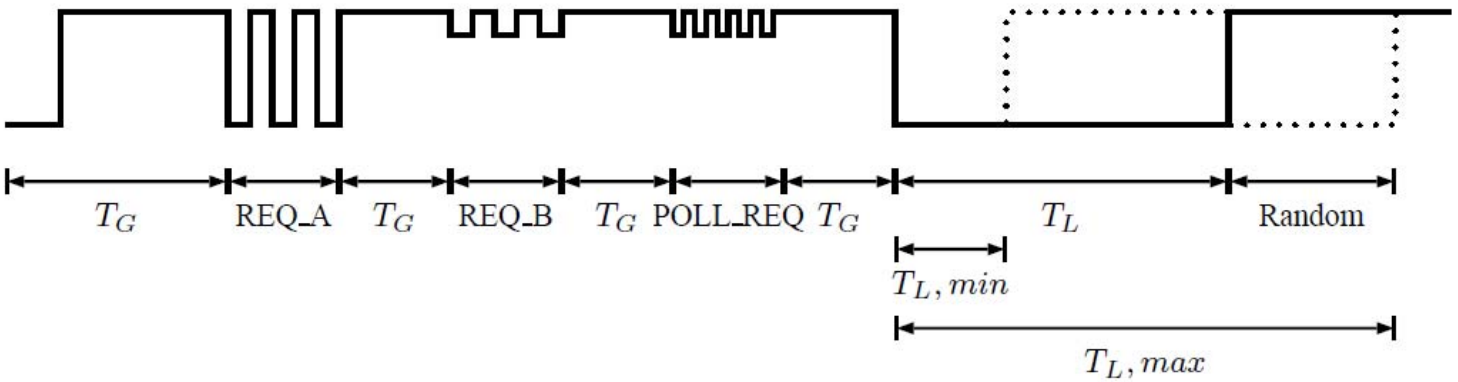
Requirements:

- Low power consumption
- Fast detection of peer devices
- Reliable advertising of presence
- Collision prevention
- Support of all required smart-card standards:

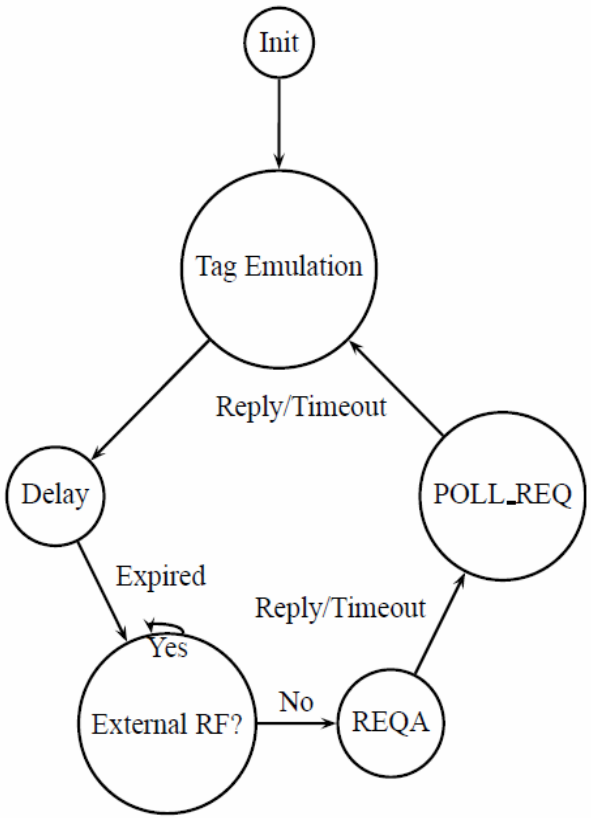
  ISO-14443A, ISO-14443B, Felica, Jewel, My-D, NFC-Forum Tags, etc…

Mode Switch (3)

Suggested sequence of commands: Mode Switch requests cards to detect them



Implementation



- „Eternal“ cycle of request commands
- Tag emulation persists at least for the delay time, longer if external field detected
- ISO 14443-3A
- Felica
- NFC-devices will stay in mode when requested

Possible issues

- Incompatibility of modulation schemes
- Mode selector sensitive to RF field breakdowns
- Matching of NFCID1 and NFCID2
- Interface to higher protocol levels not yet defined

End

Questions?