Handsets, reader tools, standardisation and certification

2011-09-01

Content

telenor group

Standardisation and certification

Content

1. NFC Specifications
   - Overview
   - Specifications
2. Card emulation
   - TSM architecture
   - GSMA API
3. Programming Interfaces (API)
   - Java
   - Android
4. User Interface
5. Sectors
   - Payment
   - Transport
   - Identification
   - Access
   - Health

telenor group

NFC – Near Field Communication

- Short-range wireless connectivity for electronic devices (such as a mobile)
  - Standardised
  - Range < 10 cm
  - 13.56 MHz
  - 106, 212, 424 kbit/s
  - No battery (in tags)

- Reader/writer mode
  - Use the mobile to read/write tags
  - Mobile as a POS terminal
- Peer-to-peer mode
  - Use the mobile to interact with another mobile or electronic device
  - Phone to phone transactions
- Card emulation mode
  - Use the mobile as a tag for external readers
  - Mobile as a payment card, ticket etc.

telenor group

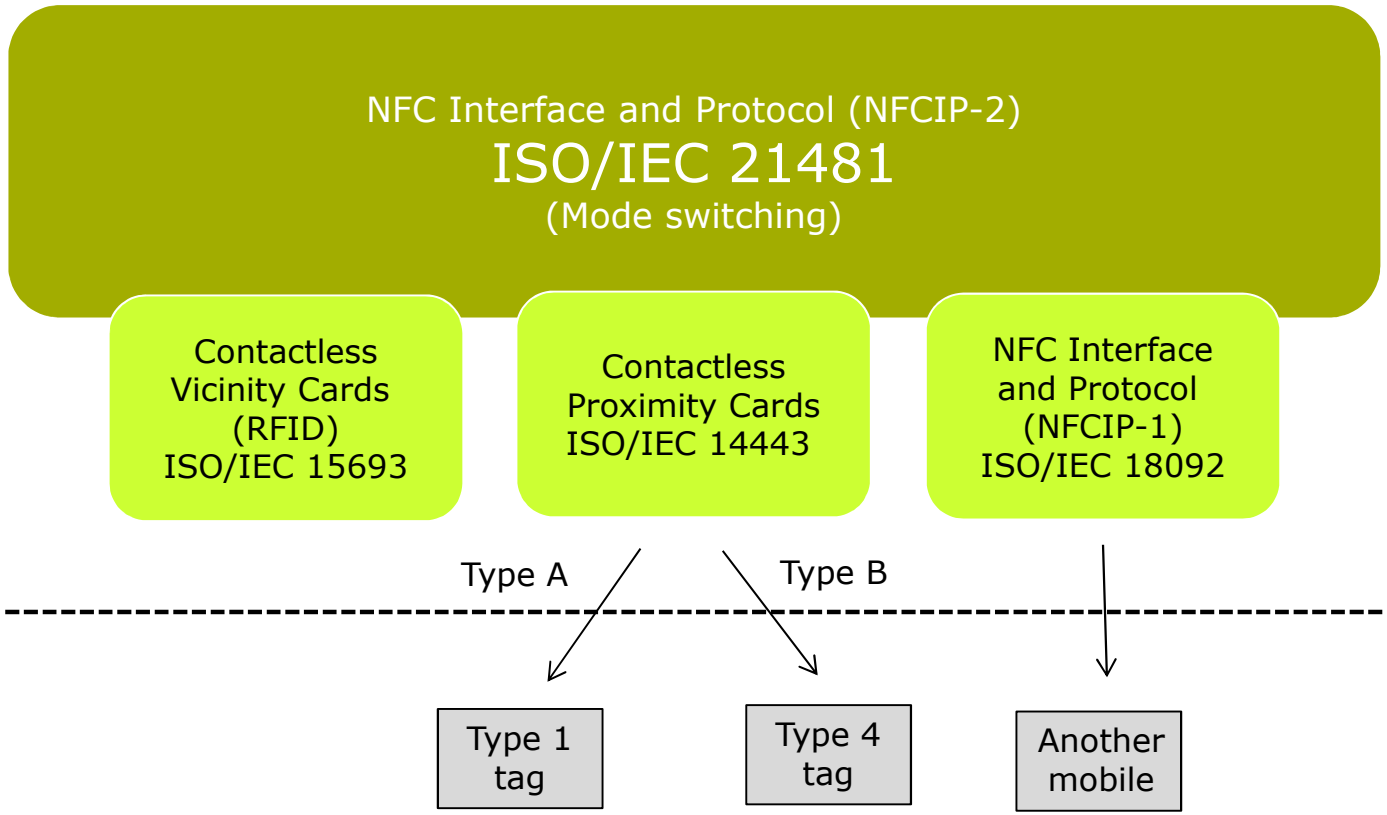
NFC Standards (1)

- ISO/IEC 14443 (Contactless Integrated circuits cards, proximity cards)
  - Standardizes physical characteristics, radio interface, initialization /anti-collision and transmission protocols
  - Type A & B depending on radio interface
- ISO/IEC 15693 (Contactless Integrated circuit cards, vicinity cards)
  - RFID item tracking
- ISO/IEC 18092 or ECMA 340 (Near Field Communication interface and protocol, NFCIP-1)
  - Standardizes RF field/signal interface, initialization /anti-collision and transport protocols
  - Active and passive RF modes, peer-to-peer mode
  - Several data rates
- ECMA 351 / ISO 21481 (NFCIP-2)
  - Specifies operation mode selection (ISO 14443, 15693 of NFCIP-1)
- JIS 6319-4 (FeliCa)
  - Contactless card

telenor group

NFC Standards (2)

- Selection of correct communication mode



telenor group

NFC Standards (3)

- NFC Data Exchange Format (NDEF) Technical Specification
  - Common data format for NFC compliant devices and tags
- NFC Forum Tag Type
  - Type 1 : based on ISO/IEC 14443 A. Read/re-write, 96 – 2k byte
  - Type 2: based on ISO/IEC 14443 A. Read/re-write, 48 – 2k byte
  - Type 3: based on JIS X 6319-4 (FeliCa). Read/re-write/read-only, up to 1M byte per service
  - Type 4: fully compatible with ISO/IEC 14443, both A and B. Read/re-write/read-only, up to 32k byte per service
- NFC Record Type Definition (RTD) Technical Specification
  - Well-known types
    - Text, URI, Smart Poster
- NFC Generic Control RTD Technical Specification
  - A way to request a specific action (starting an application, setting a mode) on a NFC device
- NFC Signature RTD Technical Specification
  - Signing of NDEF records (several algorithms/certificates supported)

telenor group

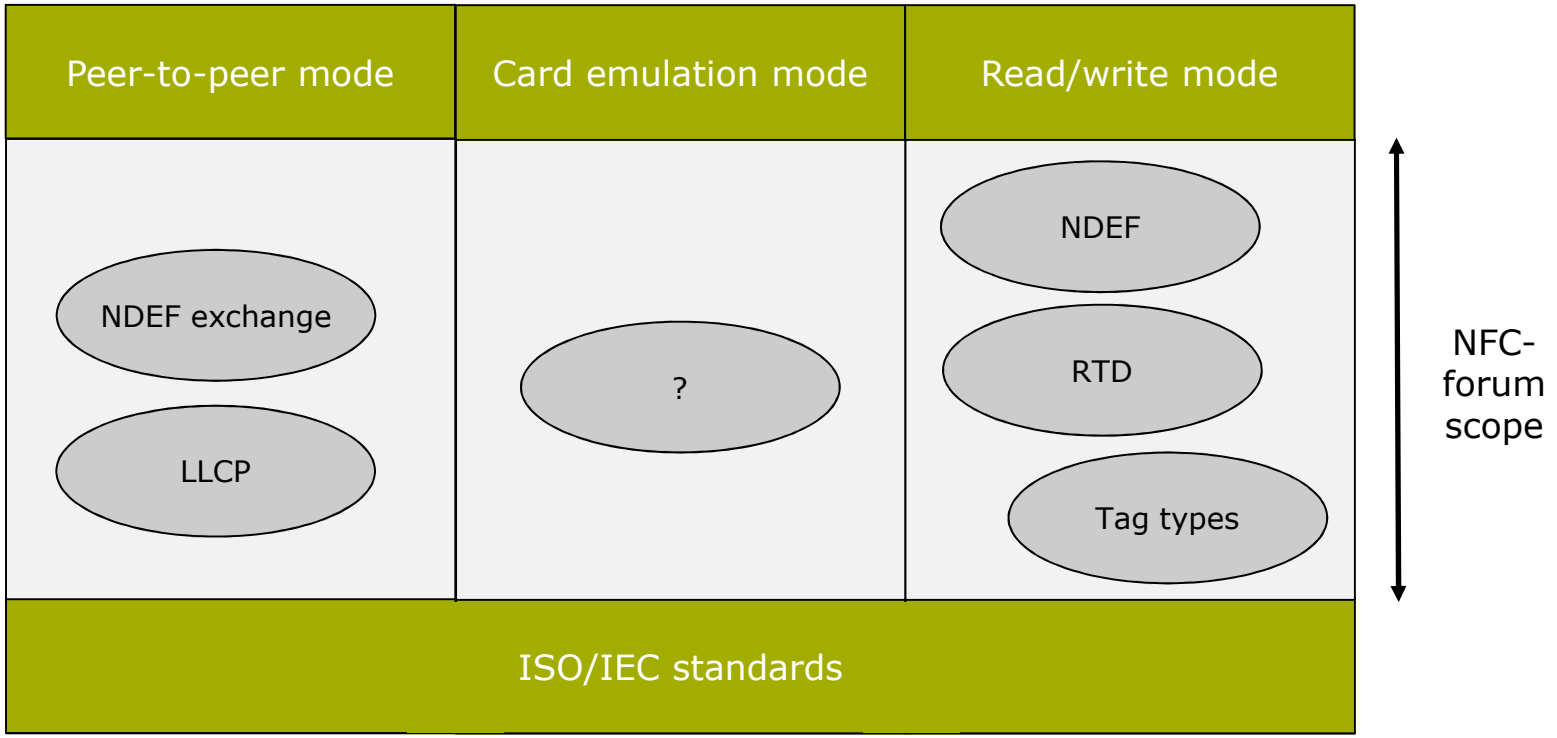
NFC Standards (4)

- NFC Logical Link Control Protocol (LLCP) Technical Specification
  - OSI Layer 2
- NFC Digital Protocol Technical Specification
  - Showing developers how to use NFC

telenor group

NFC Standards (5)

- Builds on ISO/IEC standards

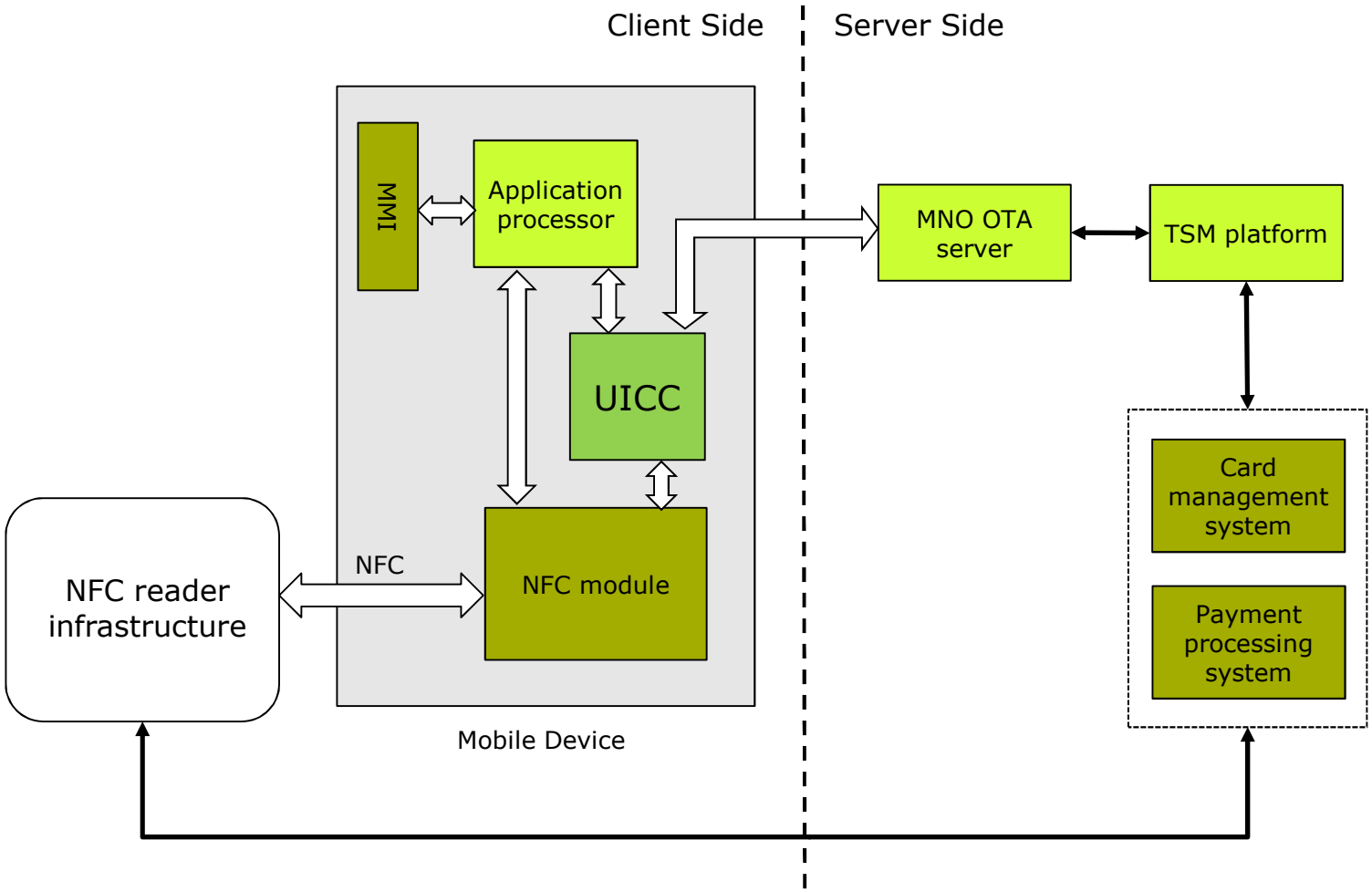


NFC Forum – Marks and Certification

- NFC Forum provides two types of marks (or logos)
  - N-Mark – Universal symbol for NFC. Signals that a NFC service is available. Symbol and guidelines for its use can be downloaded from NFC Forums web page
  - Certification Mark – Means that a product has passed NFC Forums certification testing
- Certification Program
  - Ensures interoperability between devices
  - Compliance with the NFC Forum specifications
  - Organised in two “waves”:
    1. 2010 – only provides certification of a subset of layers
    2. 2012 – program extended to include more layers
  - Certification handled by a third party (The Open Group)
  - Certified products will get the Certification Mark

telenor group

Card emulation - architecture



Card emulation (1)

- ETSI TS 102 613 – Single Wire Protocol (SWP)
  - Covers communication at the hardware level between UICC (SIM) and Contactless Front-end (CLF)
  - Similar to SPI/I2C/1-wire
- ETSI TS 102 622 – UICC-Contactless Front-end interface, Host Controller Interface (HCI)
  - Defines an API on top of SWP
  - Routing
- 3GPP TS 11.11 SIM-ME interface/ETSI TS 102.221 UICC-Terminal Interface
  - ISO 7816 based communication
- 3GPP TS 11.14 SIM application toolkit/ETSI TS 122.038 USIM application toolkit/ETSI TS 102.223 (Card Application Toolkit)
  - Proactive commands (allows UICC to take initiative)
  - Simple MMI interface
- OMA SmartCard Web Server (SCWS)
  - Access to web-pages on UICC or ”push” of web-pages from UICC

telenor group

Card emulation (2)

- Global Platform Card Specification (GP)
  - Security domain creation and management of applets (application) on a UICC or secure element
  - Secure channel protocols (SCP)
  - Commands for secure application download/install/delete/lock etc.
- 3GPP TS 03.48/ETSI TS 102.225/226
  - Remote file management of a UICC (RFM)
  - Remote application management of a UICC (RAM)
  - Aligned with GP command set
- TSM and OTA infrastructure (TBD)
  - Work on specifications currently done within Global Platform
  - GSMA

telenor group

Programming Interfaces (API)

- Currently two environments
  - Java J2ME
    - New APIs are created in form of Java Specification Requests (JSR) within the Java Community Process (JCP)
  - Android
    - Whomever Google chooses to work with
- Read/write and peer-to-peer mode
  - J2ME
    - JSR257 – Contactless Communication API
  - Android
    - `android.nfc.*` (available from rel. 2.3 on - API Level 9)
- Card emulation (i.e. access to UICC/Secure Element)
  - J2ME
    - JSR177- Security and Trust Services API for J2ME
  - Android
    - Currently no official API, but work is being done through the SEEK initiative

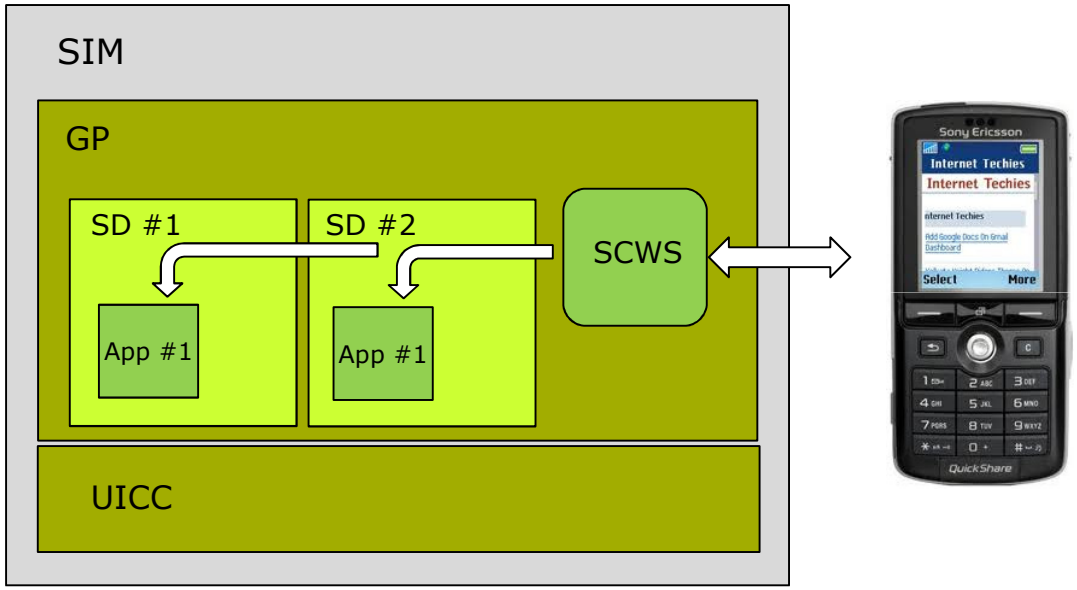
      http://code.google.com/p/seek-for-android/

      Ver. 2.1.1: Compliant with SIMAlliance Open Mobile API Specification

telenor group

User interfaces (1)

- OMA Smart Card Web Server (SCWS)
  - HTTP 1.1 Web Server embedded in a Smart Card or in a SIM card
  - OMA SCWS v.1.1 Technical Specification



  - Can act as a intermediate providing user interface to applets on SIM
  - Requires support for SCWS on terminal

telenor group

User interfaces (2)

- User interfaces can also be provided as an application on the handset, acting as a front-end for the applet on the SIM
- A prerequisite is access to an API that provides access to the SIM
- Alternatives:
  - Open Mobile API
    - Developed by SIMalliance
    - General API for providing access to SIM (UICC), embedded Secure Elements (SE) and Secure Memory Card
    - For Android the SEEK initiative provides a compliant API

      http://code.google.com/p/seek-for-android/
  - Java (J2ME)
    - Primarily for mid-range handsets
    - JSR 177 – Security and Trust Services API
    - JSR 257 – Contactless Communication API

telenor group

Sectors - payment

- Debit and credit solution must generally be compliant with and certified according to the EMV specification
  - Stands for EuroPay, MasterCard and Visa
  - Specification maintained by EMVco
  - ISO/IEC 7816 for contact cards and ISO/IEC 14443 for contactless
- Known EMV implementations
  - VSDC (Visa), MChip (MasterCard), AEIPS (AmEx), J Smart (JCB)
- EMV compliant contactless cards
  - Visa: Visa Wave, payWave, Quick VSDC, Visa Contactless
  - MasterCard: PayPass
  - AmEx: ExpressPay
  - Discover: Zip
- Should be possible to move solutions to an NFC environment, but there might be issues with moving from an one-vendor environment to a multi-vendor environment.
- Paypal
  - Has recently announced a NFC payment solution on Android handsets

    http://venturebeat.com/2011/07/13/paypal-android-nfc/

telenor group

Sectors - transport

- Ticketing solutions are typically regional
- Given the need to be able to move between different means of public transports, ticketing solutions are sometimes defined by the local authorities
- National Transport Plan - Norway
  - Håndbok 206 (HB206)
  - Maintained by Vegdirektoratet
  - De facto standard for electronic ticketing
  - Currently specifies DESFire as contact-less technology
  - Under revision, NFC is considered
  - Infrastructure an issue

telenor group

Sectors - identification

- MinID – http://minid.difi.no/
  - Public ID (Norway)
- Buypass – http://www.buypass.no/
  - Electronic identification, signing and payment
- Digital signature – PKCS#11
  - Primarily adopted to smart cards
  - Platform independent API
  - Handles RSA, X.509 certificates, DES/3DES tokens
  - Used for signing, encryption and verification
- NIST – Personal Identity Verification (FIPS 201)
  - Specifies Personal Identity Verification (PIV) for US Federal employers and contractors

telenor group

Sectors – access

- TBD

Sectors – health

- TBD

Content

telenor group

Handsets

Content

1. Android
2. Other

Android

Functionality of handset depends upon the version of Android used

- Ver. 2.3.3(4) – Gingerbread
  - R/W and P2P
- Ver. 4.0 – Ice Cream Sandwich
  - Expected oct. 2011
  - R/W, P2P and emulation support (SWP and SE)

Handsets on the market

  - Samsung Nexus S (Gingerbread)
  - Samsung Galaxy II (Gingerbread)
    - Only on some models

Handsets announced

  - Samsung Nexus Prime (Ice Cream Sandwich)
    - Expected oct. 2011
    - Firmware upgrade for Nexus S will be available later
- Many other handsets expected
  - SE, ZTE

telenor group

Other

Samsung

- GT-S5230N
  - R/W, P2P and emulation
- Support for R/W announced in Bada 2.0

Nokia

- C7 – has NFC support in hardware but requires a firmware upgrade
- Three Symbian handsets announced with NFC support
  - Belle

RIM

- Several models

telenor group

Content

telenor group

Reader tools

Content

1. Readers
2. Chipsets

telenor group

Readers

- Types
  - Contactless / smartcard
  - USB / Serial
- Protocol
  - PC/SC
  - Proprietary
- Requirements contactless
  - read/write
  - ISO/IEC 14443-4 (ISO DEP)
  - NFCIP-1 (peer-to-peer)
  - Proprietary: ex. Mifare Classic, etc.
    - Programmers manual
- Requirements UICC / smartcard
  - ISO/IEC 7816-3 (T0/T1)

telenor group

Chipsets (1)

- NXP - http://www.nxp.com/
  - Readers
    - PN53x series – ISO14443 A/B
  - Handsets
    - PN544 – (SWP and SE)
      - Nexus S
- Inside Secure – http://www.insidesecure.com/
  - Readers
    - PicoRead
  - Handsets
    - microread – (SWP)
      - RIM, ZTE
    - securead – (SWP)
  - Initiated the Open NFC protocol stack initiative for Android (http://www.open-nfc.org/)

telenor group

Chipsets (2)

- Infineon Technologies
  - Readers
    - SLE 66 family
  - Handsets
    - SLE 97 family
    - SLE 88 family (SWP)
- STMicroelectronics
  - Handsets
    - ST21NFCA (SWP)
- Sony
  - FeliCa
- Texas Instruments
  - Readers
    - TRF7960
    - TRF7970A

telenor group

Chipsets (3)

- Renesas
  - Handsets
    - RF21S (R/W, P2P and SWP)
- Samsung
  - Has announced a chip for handsets with mass production starting in 2011

telenor group

Content

telenor group

Working with NFC on the lab

Equipment and tools needed for working with NFC

- Readers – low level access
- J2ME
- SIM / UICC and Secure Element
- Android (briefly)

telenor group

Readers – low level access

- Adafruit Industries

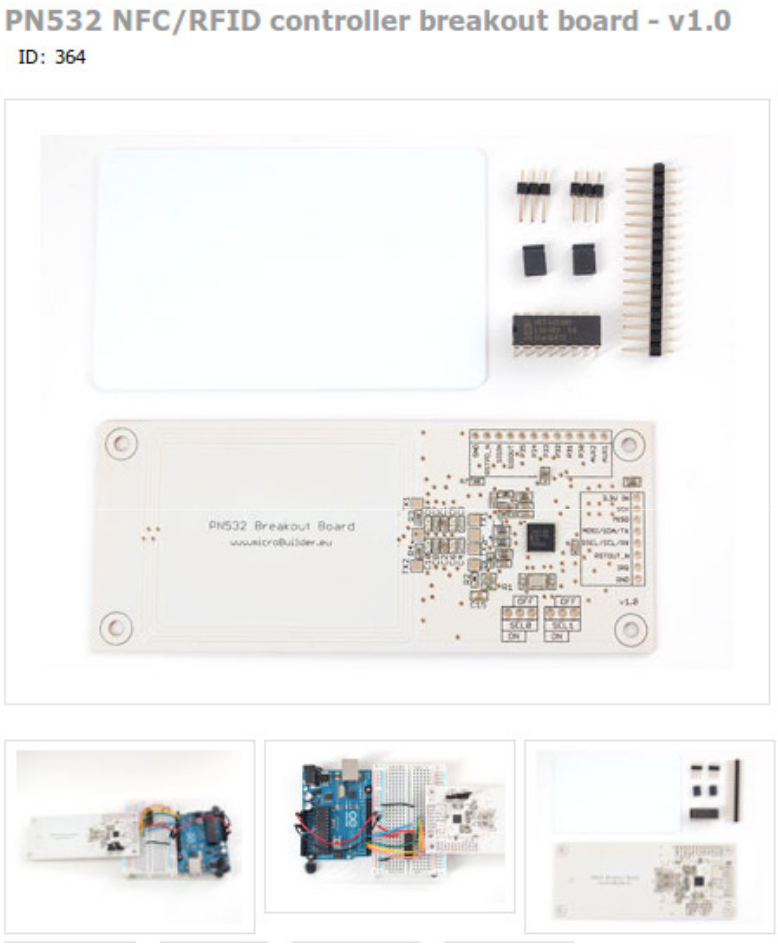
  http://adafruit.com/

- NXP PN532 NFC chip
  - ISO 14443 A/B
  - NFCIP-1 mode (peer-to-peer)
  - Mifare Classic / Sony FeliCa
- Can be used as a NFC reader using the libnfc library

  http://code.google.com/p/libnfc/

- Usable for standalone (embedded) solutions
- Target is the hobbyist market
  - USD 50
- Other examples exists

  http://www.openpcd.org/



telenor group

Development with J2ME (1)

- Application (MIDlets) that uses the JSR 257 and JSR 177 APIs
  - Read/write
  - Peer-to-peer
  - Access to SIM / Secure Element
- Handset vendors that supports NFC (Nokia, Samsung) has development tools and/or SDK that can be downloaded and used for free
  - Nokia Series 40 SDK for Nokia 6212 NFC and Nokia 6131 NFC
  - Nokia Symbian^3 SDK w/NFC plugin for Nokia C7
- Can also use Sun (now Oracle) Java ME SDK and add JSR 257 / JSR 177 libraries from an vendors SDK if not already present
  - Disadvantage: emulation might not work (debug on device)
- Tools required
  - SDK
  - Handset, tags
  - 3rd party signing certificate
- Signing certificate
  - Thawte, VeriSign – typical cost: USD 200-300 per year
  - Self signing might work

telenor group

Development with J2ME (2)

- Installation of J2ME MIDlets, use either cable or download “over the air” using the “Antenna” tool:

  `http://antenna.sourceforge.net/`

- Programming of tags
  - Easiest to use the handset
  - Contactless reader supporting the tag type
    - For tags such as Mifare Classic, access to the Programmers Manual for the reader will typically be required, as the API is not standardized

telenor group

Application development for SIM/UICC and Secure Element (1)

- SIM / UICC cards
- If subscription on UICC
  - Keyset data (GP/OTA) for the cards (key file exported from DP)
- If without subscription (or with embedded Secure Element)
  - Keyset data from vendor (typically set to well-known default values)
- Development tool, preferably from a SIM vendor
  - Libraries
  - Emulator
  - Tool for uploading of applets
  - Example: Gemalto Developer Suite (cost: 1000 EUR for 2 years)
- Smart Card reader (ISO 7816-3 compatible)
- With Secure Element (SE) a Contactless reader must be used (ISO DEP compatible)
- Typical work procedure
  1. Write code in IDE tool
  2. Test on emulator
  3. Upload to UICC/SE and test

telenor group

Application development for SIM/UICC and Secure Element (2)

- Gemalto Developer Suite
  - Based on Eclipse
  - Cards
    - SIM R99/R5
    - UICC R5/R6
    - NFC with SCWS
  - Simulators
    - 2G (SMS, Call Management, Timers, etc.)
    - 3G (BIP, SCWS, etc.)
    - OTA emulation
  - Deployment
    - Application Manager for 2G/3G
- Free alternative (but without debugging or emulator)
  - Eclipse / text editor
  - Java Card 2.2 from Sun and SIM API signature files from ETSI Java API specifications
  - SIMAlliance CAT Loader Tool
  - Alternative: Gpshell (`http://globalplatform.sourceforge.net/`)

telenor group

Android

- Supported in API level 9 (ver. 2.3) or newer
- Currently supports
  - read/write and peer-to-peer(?)
  - NFC-A, NFC-B, NFC-F, NFC-V, ISO-DEP
  - NDEF tags
  - Mifare Classic and Ultralight
- Handsets
  - Samsung Nexus S
  - Samsung Galaxy II (NFC currently not enabled)
  - Many others coming
- Access to SIM currently only possible using the emulator connected to a smart card reader with the SIM inserted
  - The SEEK initiative:

    http://code.google.com/p/seek-for-android/
- Full supports on handsets requires that vendors updates the RIL (Radio Interface Layer) firmware on their handsets to support access to SIM and enables BIP (if SCWS is to be used)

telenor group