The Potential of SIM Cards as an Application Platform for Smart Server Systems

Gerald Madlmayr

NFC Research Lab, Hagenberg

Smart Mobility 2008, Sophia Antipolis

www.nfc-research.at
NFC Research Lab Hagenberg

- Research Topics
  - Software: Contactless Applications and Infrastructure
  - Hardware: Testing & Interoperability
  - Security
  - Usability

- Founded by Industry Partners
  - Mobilkom Austria (Vodafone Partner)
  - NXP Semiconductors
  - Omnikey/Assa Abloy (HID Global)

- NFC Forum Member
Potential of SIM/UICC

- SIM/UICC considered as Secure Element for NFC
- UICC as a multi application platform (JavaCard based)

Applications
- GSM/UMTS Application
- the Wireless Identity Module (WIM), based on PKI
- VAS applications through the SAT technology
- Contactless Applications

Space
- 128 K – 256 K
- Applet: Mastercard’s PayPass ~ 20 K
SIM Approach in NFC

- SIM Application Tool Kit (SAT)
- SIM Card uses Data Services of Handset (BIP)
- SIM Card acts a contactless reader
- Communication with other Secure Elements
  - NFC HCI defines pipes between secure elements
  - Management of other secure elements by TSM
SIM Application Toolkit (SAT)

- “Everything” running on the SIM
  - Application
  - GUI
  - OTA Connection

- Evaluation
  - + does not depend on handset/OS
  - - limited GUI/interaction
  - - only for SIM Card
SAT Development today:

- Dev-Tools needed (HW & SW)
- “open”, but provisioned SIM Card
- Development about 3 – 5 x (comp. to J2ME)
- Small Community, few documents, few tutorials
- Example: Socket Connection
  - J2ME: 50 Lines of Code; 100+ Examples on the Web; 1 h Work
  - SIM: 400 lines of Code; 1 Example; 1 Week Work
Bringing two Worlds together

- SmartCard Webserver
  - Smartcard Engineers develop Servlets?
  - Web developers go contactless?

- Imagine …
  - Click on a Web link causes to phone to read a Tag
  - Local “MasterCard Servlets” for mobile Payment
  - Your Handset is your FaceBook
  - Web sites make use of “localhost” Content (Web 2.0)
  - IP over NFC for external RF communication
  - SOAP based Services on SIM
Building a light weight SIMServer

- **Recipe**
  - OMA SCWS Standard (Final Release April ’08)

- **Ingredients**
  - BIP SIM-Card
  - SAT Developer Tool
  - Emulator/Handset

- **Preparation**
  - Stir well and invest some time
Basic Functionality: BIP Client Mode

- UICC sends BIP comments to BIP Gateway (1)
  - „Establish an IP Connection to …“
- BIP Gateway (2)
  - TCP/IP Channel is setup (GPRS/EDGE/UMTS)
SCWS Functionality: SCWS Remote Management

- Short message is sent to handset (1)
- Card Admin agent is triggered (2) and advises BIP Gateway to establish a connection (3)
- Remote Server receives client request (4) and is able to send data to the SCWS
- Other triggers (@ 1): Time, User Interaction (Open App, Touch Tag/NFC …)
Basic Functionality: BIP Server Mode

- BIP Gateway sends Request for Connection (1)
  - TCP/IP Stack can offer a Server Socket
- Browser is able to contact "localhost" (2)
  - Send HTTP/HTTPS Request to UICC
SCWS Functionality: Local Access

- TCP/IP Stacks offers Socket Server Port; Browser sends request (1)
- Access Control Policy: Is application allowed to do so? (2)
- Request is forward to SCWS (3), response generated and sent back to Browser (4) & (5)
Implementation of light weight SIMServer: Status

- Supports
  - SCWS Administration Mode
  - SCWS Local Browsing Mode
  - HTTP 1.0
  - Emulator only so far/SingleThreaded
  - JavaCard 2.1

- No (yet) considered
  - ACP Enforcer
  - HTTP 1.1
  - Test on handset/real SIM
OMA SmartCard Web Server: Status Today

- Your “mobile” localhost
- Look depends on Browser
  - x different Display sizes
  - y different mobile Browsers
- Multi Threaded Operating System on SIM
- Standards
  - OMA Standard (for JC 2.1)
  - Part of Java Card 3.0
Smart Card Web Server: Pros & Cons

- Access through
  - NFC/RF
  - OTA
  - Application on handset (Browser)

- Evaluation
  - + nice web interface to Applications on the SIM (also phonebook, …)
  - +/- SIM bigger and more expensive
  - - Browser/special Handset needed
  - - User Experience: GUI/UE not satisfying
SmartCard Web Server (SCWS): Usecases

- MNO/Handset Manufacturer: Branding of Browser
- On-Card Portal as „Home“ in Browser
- Local/Remote File Administration on SIM
- Hot-Deployment of Application OTA of
  - CardLets
  - Contactless Applications
- Images, CSS and Templates on SIM (Space!)
Conclusion

- SIM become a complex and flexible application platform

- SCWS on JC 2.1
  - Not multi threaded
  - High development effort

- JC 3.0: MIDP/CLDC Functionality in a SIM

- Space on SIM costly (Graphics, Animations)

- Deployment requires TSM or MNO
Near Field Communication
Research Lab
Hagenberg

NFC Congress 2009
24 – 26 February
Hagenberg, Austria
congress.nfc-research.at

Happy to answer any questions
Gerald.madlmayr@fh-hagenberg.at
http://www.nfc-research.at