
SmartMX, NFC & Arygon

Ralf Kretschmann, Achim Kretschmann, Bernd Fleischmann



SmartMX und NFC Technik - Arygon

Gliederung

- Projektarbeit

Integration des Philips SmartMX Controllers in Arygon NFC Produkte

- Grundlagen & Motivation
- Anforderungen
- Architektur
- Zusammenfassung

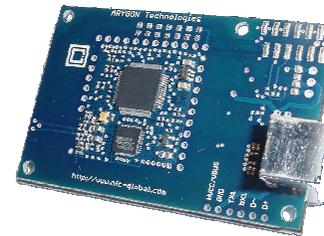
- NFC Technologie & Demo

- NFC Anwendungsgebiete & Märkte

SmartMX und NFC Technik - Arygon

Grundlagen

- Arygon Technologies AG 
- Vertrieb von RFID Produkten
- Eigene Entwicklungsabteilung für NFC Produkte
- Eigenentwicklungen
 - NFC/ Mifare Reader Modul APPA
 - Handys AMPA, APDA



SmartMX und NFC Technik - Arygon

Definitionen

- NFC - **N**ear **F**ield **C**ommunication
„Weiterentwicklung von RFID“ – ISO18092
→Peer-to-peer aktiv-aktiv Modus

- ISO7816 - Norm für Smart Cards
 - Enthält physikalische und elektrische Anforderungen: Teil 1-2
 - Beschreibt Kommunikationsschichten und Softwareschnittstelle: Teil 3-15

- ISO14443 - Norm für kontaktlose Chipkarten = ISO7816 kontaktlos

- SmartMX - Philips SAM (Security Authentication Module) µController
 - Security Memory, Java Card konform, ISO14443 Schnittstelle, Mifare

- Mifare - Philips Verschlüsselung zur Speicherung und Übertragung von Daten bei kontaktlosen Karten
 - Basiert auf ISO14443-3
 - **Keine Norm** → nicht von ISO 14443 Readern lesbar

Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar

SmartMX und NFC Technik - Arygon

Ziel

Vision: Handy als **das** Kommunikationsmittel der Zukunft

NFC-Handy mit Mifare als „*Transponderkarte mit Display*“

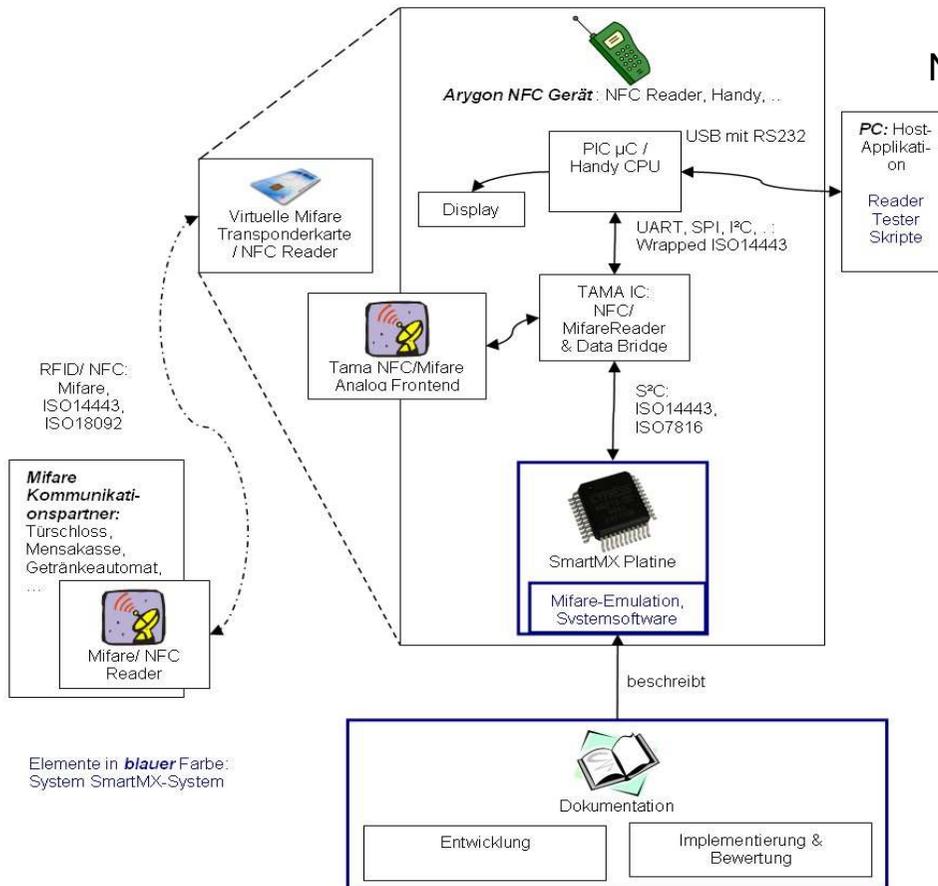


Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar

SmartMX und NFC Technik - Arygon

Gesamtsystemarchitektur



Ziel: „Transponderkarte mit Display“

→ Realisierbarkeit untersuchen anhand Arygon NFC Reader + Philips SmartMX

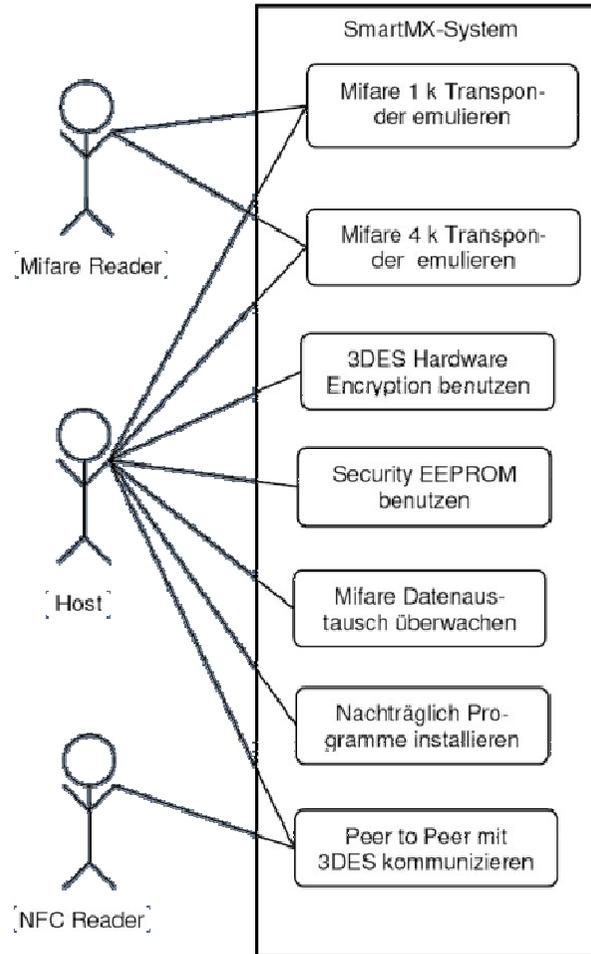


Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar

SmartMX und NFC Technik - Arygon

Anforderungen



Ralf Kretschmann, AG Robotersysteme

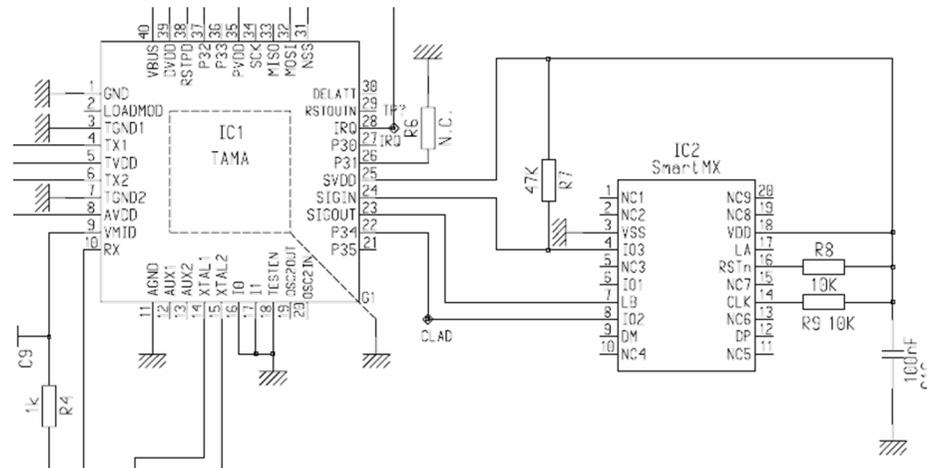
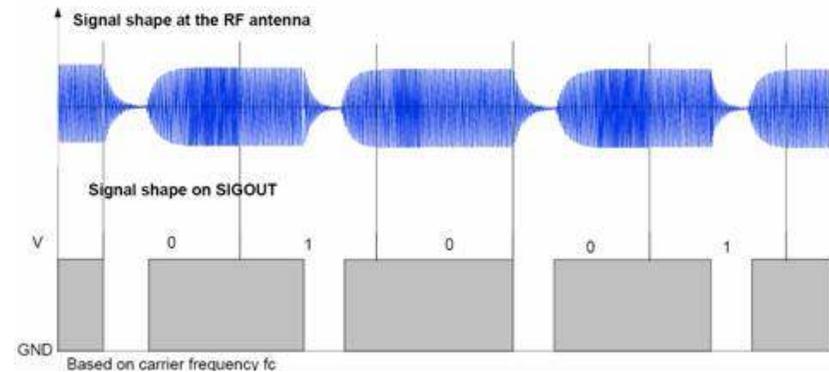
17.11.2006 Aml Mitarbeiterseminar

SmartMX und NFC Technik - Arygon

Architektur - Hardware

- Verbindung Tama - SmartMX über S²C
 - Taktung des SmartMX über S²C Träger

- Kommunikation Host – SmartMX über
 - ISO7816 über S²C
 - APDU (Smart Card Protokoll)
 - In Tama-Befehle eingepackt (wrapped APDU)
 - Mifarebefehle über S²C



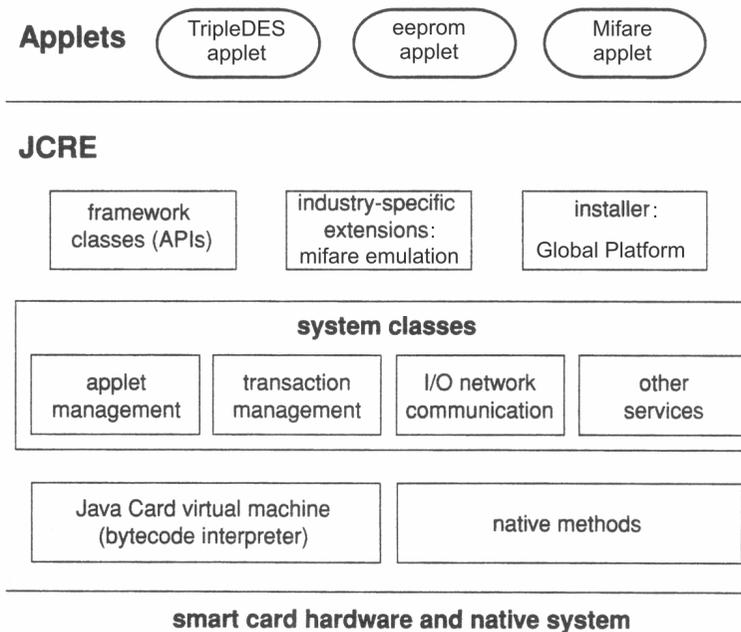
Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar

SmartMX und NFC Technik - Arygon

Architektur - Software

- SmartMX OS = Java Card Laufzeitumgebung + Global Platform Card Manager
- Card Manager: Installation von Anwendungsprogrammen (Applets)
- Java Card RE: Ausführung von Applets, Hardwareabstraktion, Kommunikationssystem (Abbildung APDU auf S²C)
- SmartMX verhält sich wie eine Smart Card nach ISO7816, Java Card 2.2.1, Global Platform 2.1.1



Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar

SmartMX und NFC Technik - Arygon

Zusammenfassung

Anforderungsrealisierung

- ✓ Mifare Transponderkarte emulieren: Entweder 1k oder 4k; beide Emulationen zusammen auf einem SmartMX ist nicht von Philips lieferbar
- ✗ 3DES Hardware Encryption benutzen (für DESFire Reader)
 - TripleDES Applet funktioniert, aber Tama schaltet im Wired Card Mode das Analog Frontend ab → Keine Kommunikation mit DESFire Transponderkarten möglich. Laut Philips keine Lösung bekannt.
- ✗ Peer to Peer mit 3DES kommunizieren: Gleiches Problem mit Tama
- ✓ Security EEPROM nutzen: Funktioniert
- ✓ Mifaredatenaustausch überwachen: Funktioniert über Applet oder einfacher über gewöhnliche Mifarebefehle im Wired Card Mode
- ✓ Nachträglich Programme installieren: Im NFC Reader: Kontaktlos mit Emsquares Reader und Entwicklungsumgebung, nicht über Reader Tester.

Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar

10

SmartMX und NFC Technik - Arygon

Zusammenfassung(2)

- Größte Probleme nicht technisch sondern organisatorisch

Kompetente Ansprechpartner, Lizenzen, HW bei IBM und Philips finden

- Expertise aus unterschiedlichen Domänen nötig

ISO7816 (Smart Card) Norm, Java Card Spezifikation, Java Programmierung, Java Card Programmierung, Java Card API / OS, Entwicklung in Eclipse, IBM JCOP Tools, Arygon/ NFC Hardware, EAGLE, NFC, Mifare, TAMA Befehle, Reader Tester Scripte, ...

- Literatur

- Chen: Java Card Technology for Smart Cards
- Spezifikationen (ISO, Java Card)
- Datenblätter zu ICs

Ralf Kretschmann, AG Robotersysteme

17.11.2006 Aml Mitarbeiterseminar