CSI/Cnlab Herbsttagung

Einführung Short Distance Communication (BLE, NFC) und SMS

Bluetooth Low Energy (BLE)

- Teil von “Bluetooth Smart Technology”
  - Frequency-Hopping-Funk
  - 0.27 MBps Durchsatz
  - Bis 100 m Reichweite
- Anwendungen
  - In allen modernen Smart-Phones vorhanden
  - iWatch, Android Wear
  - Verbindung mit Lesern (Kassen, Türen)
  - Beacons (http://blog.sbb.ch/app-mein-bahnhof/)

BLE: Security Facts

- Verbindungen können chiffriert werden
  - 128 Bit AES mit “Long-Term-Key” (LTK)
- Das Pairing ist kritisch
  - Vereinbarung des LTK mit “Temporary Key” (TK).
    - “Just works”: TK = 0 (fix)
    - 6-Digit-PIN: TK hat 1 Mio. Varianten
    - “Out-of-Band Key” hat 2^{128} Varianten
  - Cracker-Werkzeuge sind erhältlich für das Pairing

https://lacklustre.net/bluetooth/Ryan_Bluetooth_Low_Energy_USENIX_WOOT.pdf

Near Field Communication (NFC)

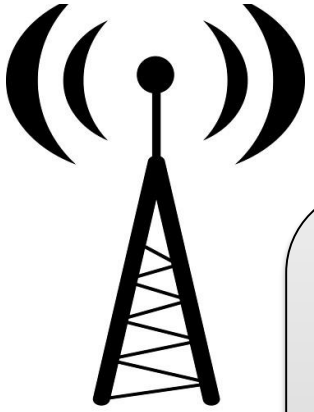
NFC ist eine Erweiterung der RFID-Technik, die sich auf kurze Strecken (max.10cm) und auf sichere Datenübertragung spezialisiert hat.

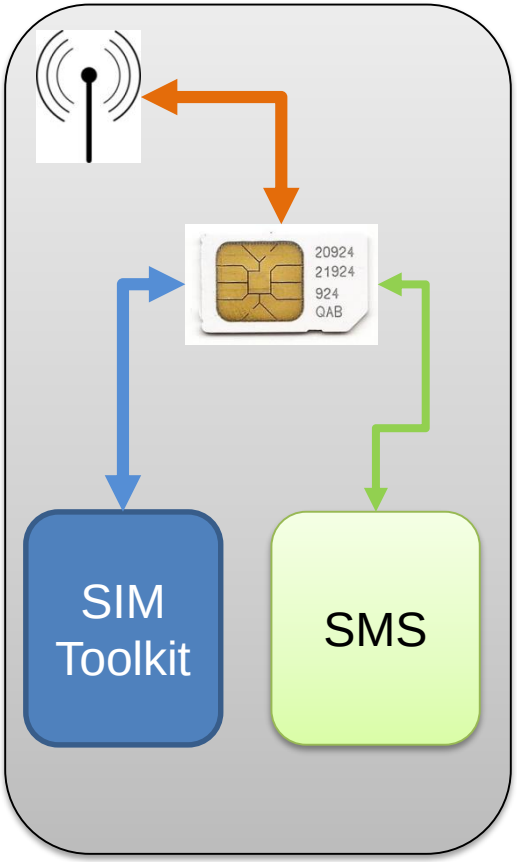
http://www.nfcworld.com/nfc-phones-list/

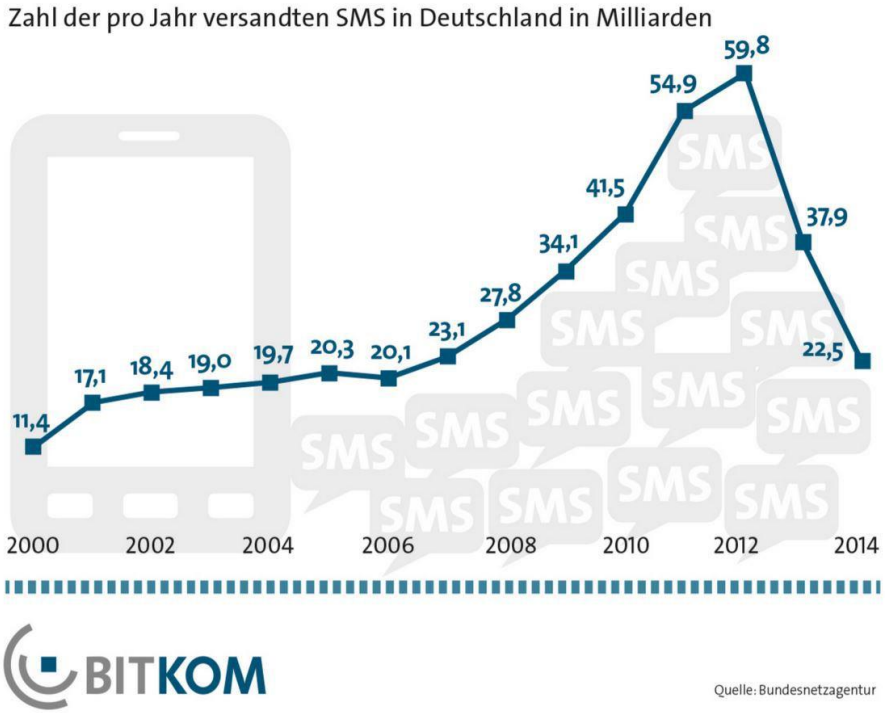
NFC: einige Facts

- Passive Transponder
  - Speisung über das Magnetfeld des Lesers
- Seit einigen Jahren im Markt
  - Zutrittskontrolle und Service-Automaten
  - Seit kurzem auch Authentisierung
  - Mehrere Standards
  - Rückwärtskompatibilität erzwingt Kompromisse
- Symmetrische Kryptologie
  - Rechenzeit-Gründe
  - Verlangt guten Schutz der Schlüssel im Leser

Short Message Service (SMS)







SMS: einige Facts

- Schutz der Übertragung
  - Luftstrecke ist chiffriert
  - Offen beim Telecom-Provider
- Verarbeitung in Smart-Phone
  - System-App (in Android auswechselbar)
  - Spezial-Rechte für Zugriff auf SMS nötig (aber weit verbreitet)
  - Integration in Cloud-Dienste (iMessage, WhatsApp)
  - Spezialdienste (SIM-Toolkit, MobileID)

Danke

Paul Schöbi
paul.schoebi@cnlab.ch
+41 55 214 33 33