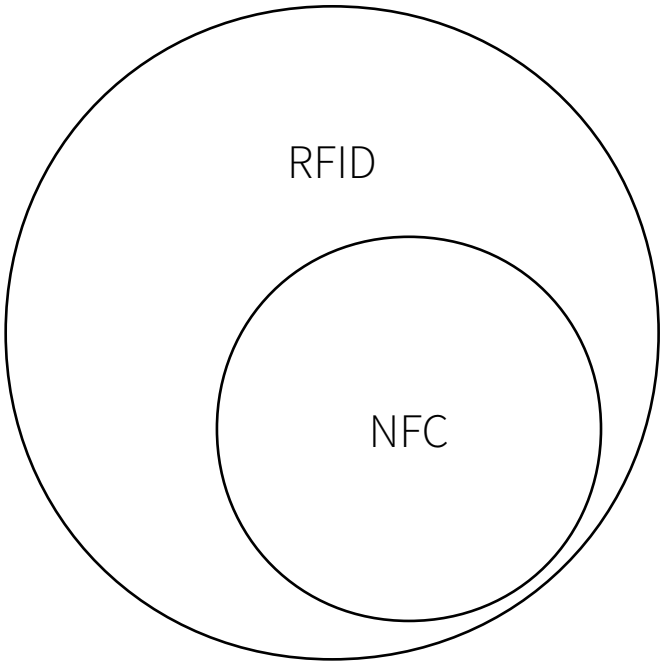
RFID/NFC-Grundlagen

Begriffe

- RFID = Radio-Frequency Identification
- NFC = Near Field Communication
- RFID ist ein Sammelbegriff für Funk-basierte Identifikation
- NFC ist ein Sammlung von Kommunikationsprotokollen (passive HF-RFID-Tags nach ISO 14443 oder ISO 15693)



Grundlegende Unterscheidungsmerkmale

- Frequenz
  - 13,56 MHz
  - 125 KHz (+/-)
  - ...
- Stromversorgung
  - Passiv
  - Aktiv

RFID/NFC-Technologien (Auszug)

13,56 MHz (NFC)

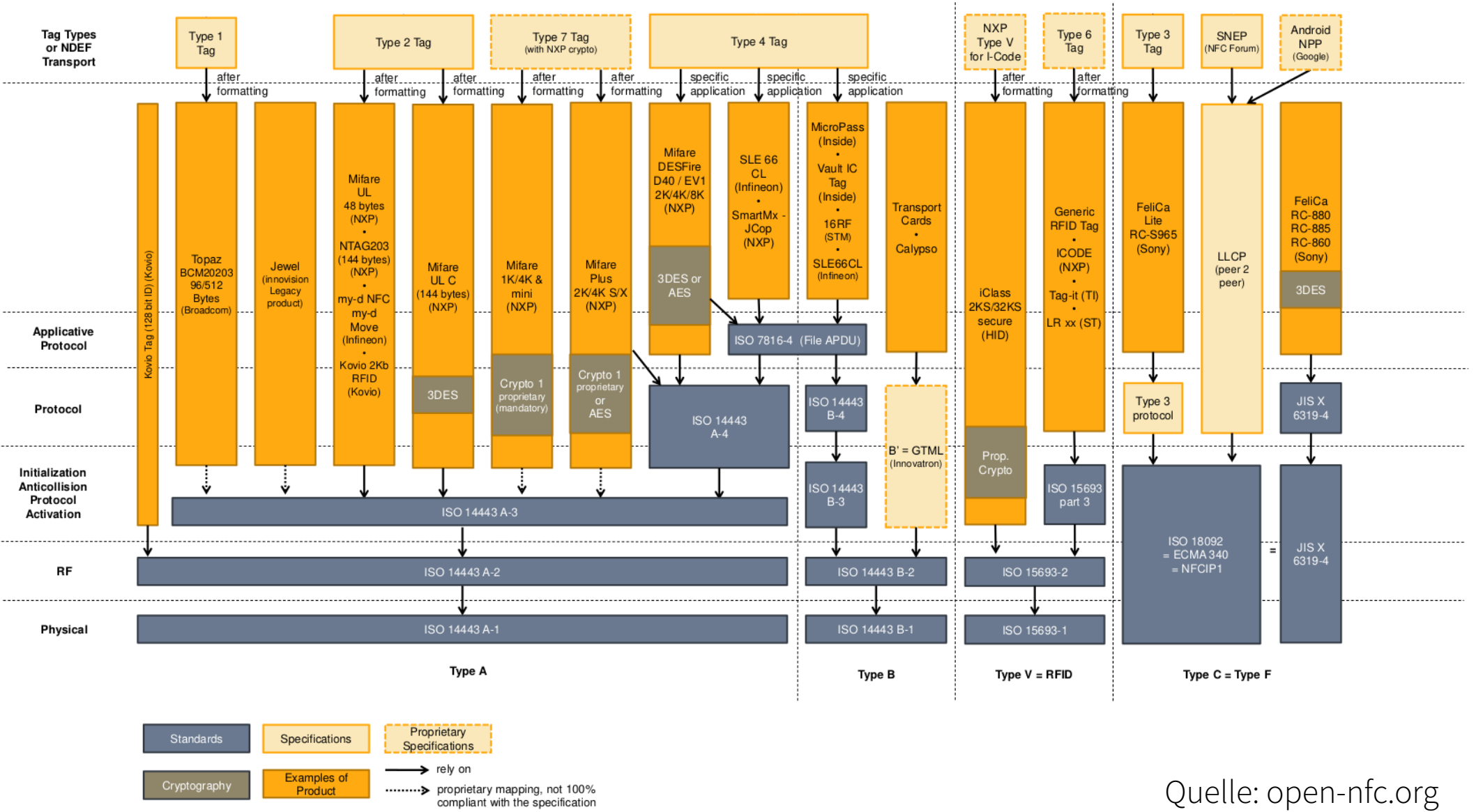
- MIFARE Classic
- MIFARE DESFire EV1 / EV2
- MIFARE Ultralight / C
- Legic Prime / Advant
- NTAG 203
- iClass
- Sony FeliCa
- ...

125 KHz (+/-)

- EM4xxx
- HID Prox
- Hitag 1 / 2 / S
- T55xx
- Viking
- FDX-B
- ...

NFC Tag Types

- NFC Forum Type 1
  - z. B. Innovision Topaz
- NFC Forum Type 2
  - z. B. NXP MIFARE Ultralight
- NFC Forum Type 3
  - z. B. Sony FeliCa
- NFC Forum Type 4
  - z. B. NXP MIFARE DESFire



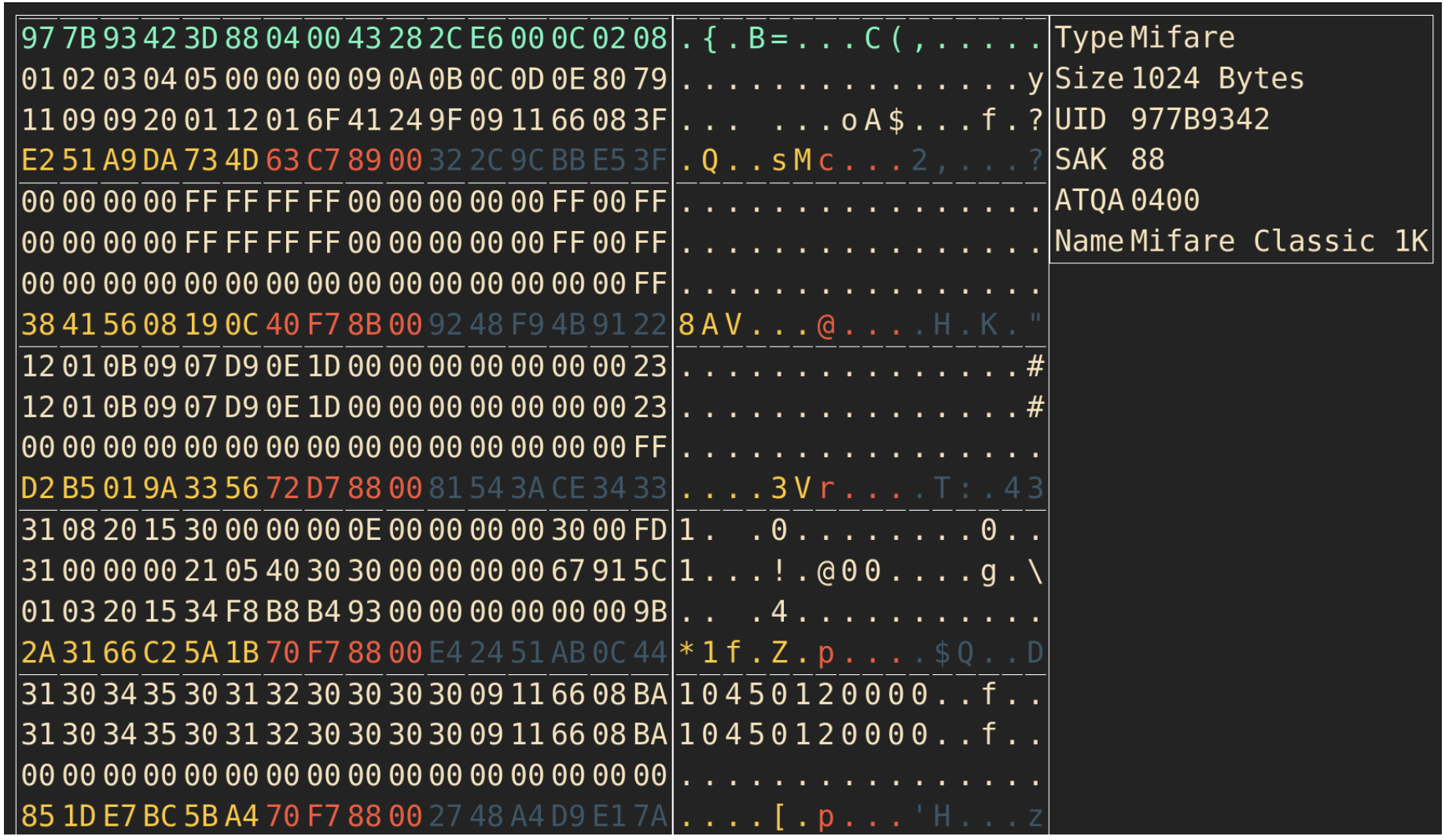
Quelle: open-nfc.org

Häufige RFID/NFC-Techniken

- MIFARE Classic
- MIFARE DESFire EV1
- LEGIC Prime
- ISO 7816-4 kompatible Smartcards (z. B. Jcop)
- (MIFARE Ultralight, MIFARE Ultralight C, EM4xxx)

MIFARE Classic

- UID: 4 Byte oder 7 Byte
- Speichergrößen: 320 B, 1 KB, 4 KB
- Organisiert in Sektoren und Blöcke
- Jeder Sektor hat zwei Schlüssel (A/B) denen Rechte zugeordnet werden können (z. B. KeyB kann Block 2 schreiben)
- Letzter Block im Sektor (Sector Trailer) beinhaltet die die Schlüssel und die Rechte (Access Conditions)
- Erster Block enthält die UID und ist Read-Only


97 7B 93 42 3D 88 04 00 43 28 2C E6 00 0C 02 08
01 02 03 04 05 00 00 00 09 0A 0B 0C 0D 0E 80 79
11 09 09 20 01 12 01 6F 41 24 9F 09 11 66 08 3F
E2 51 A9 DA 73 4D 63 C7 89 00 32 2C 9C BB E5 3F
00 00 00 00 FF FF FF FF 00 00 00 00 00 FF 00 FF
00 00 00 00 FF FF FF FF 00 00 00 00 00 FF 00 FF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF
38 41 56 08 19 0C 40 F7 8B 00 92 48 F9 4B 91 22
12 01 0B 09 07 D9 0E 1D 00 00 00 00 00 00 00 23
12 01 0B 09 07 D9 0E 1D 00 00 00 00 00 00 00 23
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF
D2 B5 01 9A 33 56 72 D7 88 00 81 54 3A CE 34 33
31 08 20 15 30 00 00 00 0E 00 00 00 00 30 00 FD
31 00 00 00 21 05 40 30 30 00 00 00 00 67 91 5C
01 03 20 15 34 F8 B8 B4 93 00 00 00 00 00 00 9B
2A 31 66 C2 5A 1B 70 F7 88 00 E4 24 51 AB 0C 44
31 30 34 35 30 31 32 30 30 30 30 09 11 66 08 BA
31 30 34 35 30 31 32 30 30 30 30 09 11 66 08 BA
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
85 1D E7 BC 5B A4 70 F7 88 00 27 48 A4 D9 E1 7A
Type Mifare
Size 1024 Bytes
UID 977B9342
SAK 88
ATQA 0400
Name Mifare Classic 1K

MIFARE Classic - Sicherheit

- Proprietärer „Crypto-1“-Algorithmus
- Seit 2008 unsicher (u. A. wegen schlechtem RNG)
- Es gibt Varianten mit verbessertem RNG
- Schlüssel können typischerweise in Minuten geknackt werden
- Tools: Proxmark3, USB-RFID-Reader, Android Smartphone, pcsc, libnfc, mfcuk, mfoc, MifareClassicTool
- Anfertigung von Clones möglich („Magic Chinese Cards“)

MIFARE Classic - Empfehlungen

- Kein MIFARE Classic verwenden!
- Migration mittels MIFARE Plus möglich
- Jede Karte sollte eigene Schlüssel haben (Schlüsselableitung)
- Reader sollten auf „Magic Chinese Cards“ prüfen
- Daten auf Applikationsebene verschlüsseln
- Daten Signieren (unter Einbezug der UID)
- Niemals nur die UID als Identifizierungsmerkmal nutzen

MIFARE DESFire EV1

- UID: 7 Byte
- Speichergröße: 2 KB, 4 KB, 8 KB
- Organisiert in Apps und Files
- Rechte auf Files werden mit App-spezifischen Schlüssel geregelt
- Verwaltung der Apps wird mit Karten-spezifischen Schlüsseln geregelt
- Teils ISO 7816 kompatibel

MIFARE DESFire EV1 - Sicherheit

- Gilt bis heute als sicher (EV2 soll noch besser sein™)
- Alte Variante (MF3ICD40) kann über Side-Channel angegriffen werden
- Optional kann eine zufällige UID verwendet werden
- „Gute Kryptografie“ (2TDEA, 3TDEA, AES)
- Mutual three-pass authentication
- Mutual authentication nach ISO/IEC 7816-4

LEGIC Prime

- UID: 4 Byte
- ISO 14443 A-1 kompatibel (Phy-Protokoll)
- Speichergröße: typischerweise 256 Byte oder 1024 Byte
- Organisiert in Segmenten
- „Master-Token System Control“ als Authentifizierungsmerkmal (Besitzt statt Wissen)

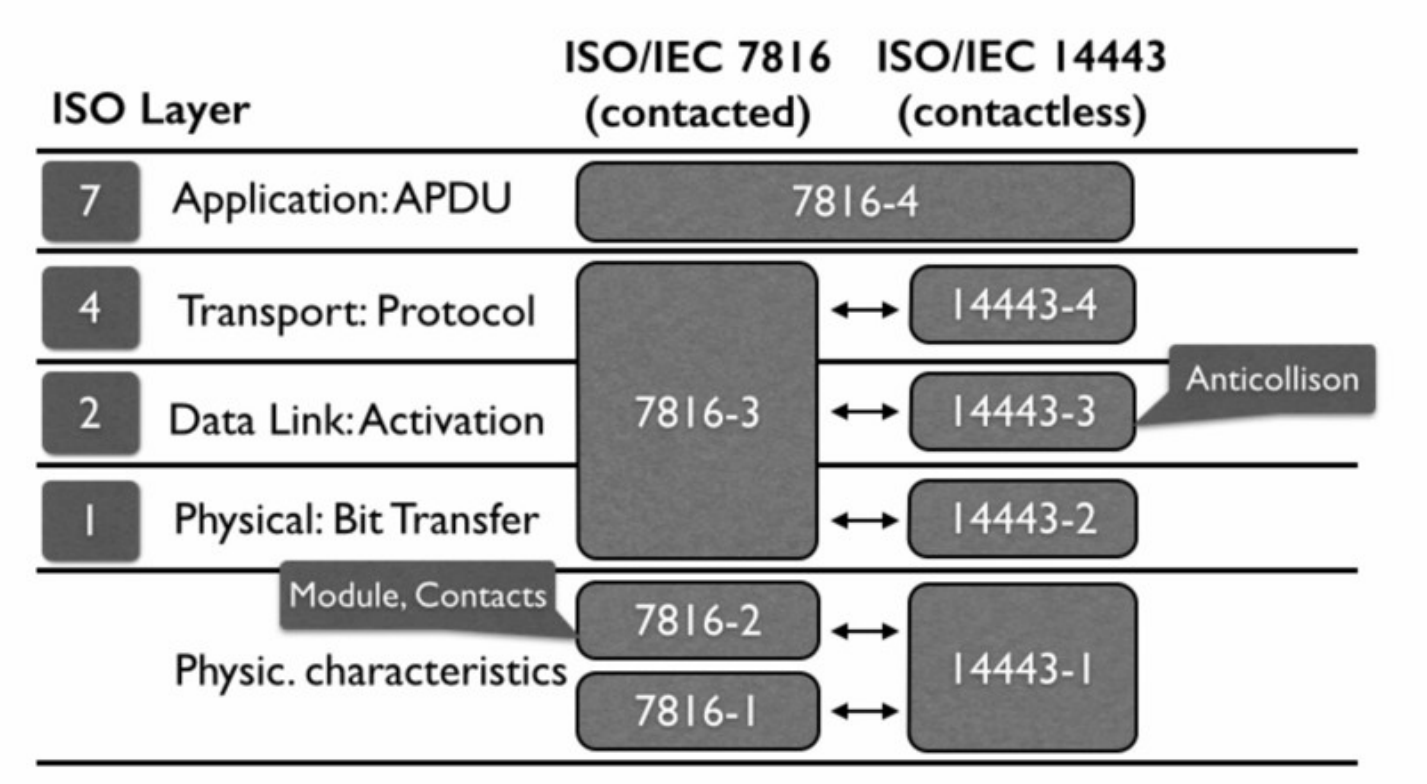
LEGIC Prime - Sicherheit

- LEGIC Prime gilt als nicht sicher
- „Obscurity in Depth“ (es gibt keine Sicherheitsmechanismen!)
- Karten können mit dem Proxmark vollständig ausgelesen werden
- Daten sind mit Prüfsumme der UID geXORt
- Kopieren von Karten ist möglich (häufig werden jedoch Segmentmerkmale und/oder die UID mit einbezogen)
- Emulieren oder clonen ist derzeit problematisch

LEGIC Prime - Empfehlungen

- Kein LEGIC Prime verwenden!
- Daten auf Applikationsebene verschlüsseln
- Daten Signieren (unter Einbezug der UID)

ISO 7816-4 kompatible Smartcards I



Quelle: blog.protocolbench.org

ISO 7816-4 kompatible Smartcards II

- Die ISO 7816-4 beschreibt ein Kommunikationsprotokoll (Application Protocol)
- APDUs zum Austausch von Daten
- Karteninhalt wird in Apps organisiert
- Karten haben häufig ein (standardisiertes) Betriebssystem
- Sicherheit ist optional

NFC Data Exchange Format (NDEF)

- Datenformat durch NFC-Forum spezifiziert
- Message (Container) & Records (MIME-Type Medien, URLs, etc.)
- Unabhängig von der NFC-Technik
- Wird u. A. von Android direkt interpretiert

RFID/NFC-Hacking-Equipment I

- Proxmark3 mit aktueller Firmware und die Möglichkeit, eine beliebige Firmware zu kompilieren
- USB-RFID-Reader (z. B. ACR-122u)
  - Software: pcsc-tools, libnfc, mfcuk, mfoc, RFIDIOt
- Android Smartphone (MIFARE Classic kompatibel)
  - Apps: NFC TagInfo, NFC TagInfo by NXP, MifareClassicTool, Scheckkartenleser NFC (EMV), NFC Card Emulator, Walrus
- Spezialkarten („Magic Chinese Cards“)

RFID/NFC-Hacking-Equipment II

- ChameleonMini (13,56 MHz, ISO14443 / ISO15693)
- 125 KHz Cloner

Fragen?