Das Vaporschloss

florolf

Entropia

6. November 2011

Anforderungen

- Schlüsseldiffusion reduzieren
  - Kopieren verhindern
  - Einzelne Schlüssel revoken
- Fallback auf Hardwareschlüssel
- Trackbarkeit verhindern

Vaporschloss Mk I

- 125 kHz RFID
- Trivial Klonbar
- Wackelige Pollin-Konstruktion
- Nicht fertiggeworden

Vaporschloss Mk II

- Mifare DESFire EV1
- Intelligentes RFID auf 13,56 MHz $\Rightarrow$
  - (hoffentlich) nicht klonbar
  - flexibler
  - Aber: Trackbar
- Fertig? (Neingeist glaubt's erst, wenn er damit die Tür aufgemacht hat)

Mifare DESFire

Sie haben gelernt

- ISO 14443-4-Kompatibel
- Gegenseitige Authentifikation (Reader $\leftrightarrow$ Karte)
- 2.5DES
- AES (Nur unter NDA)

Mifare DESFire

Sie haben gelernt

- ISO 14443-4-Kompatibel
- Gegenseitige Authentifikation (Reader $\leftrightarrow$ Karte)
- 2.5DES
- AES (Nur unter NDA)
- Naja, fast:
  - Differential Power Analysis-Attacke gegen DESFire vor EV1
    - EV1 ist EAL4+ \o/
  - Stellenweise theoretisch Replay-Attacken möglich

Was geht?

Platz

- 1, **2**, **4**, 8 kB Speicher
- Bis zu 28 Anwendungen
- Bis zu 14 Schlüssel pro Anwendung
- Bis zu 16 Dateien pro Anwendung

Was geht?

Platz

- 1, **2**, **4**, 8 kB Speicher
- Bis zu 28 Anwendungen
- Bis zu 14 Schlüssel pro Anwendung
- Bis zu 16 Dateien pro Anwendung

Dateitypen

- (Backup) Data files
- Value files
- Linear/Cyclic record files

Was geht?

Platz

- 1, **2**, **4**, 8 kB Speicher
- Bis zu 28 Anwendungen
- Bis zu 14 Schlüssel pro Anwendung
- Bis zu 16 Dateien pro Anwendung

Dateitypen

- (Backup) Data files
- Value files
- Linear/Cyclic record files

Policy

- Eindeutige UID
- Berechtigungen auf Karte/Anwendungen/Dateien

Schlüssel und Berechtigungen

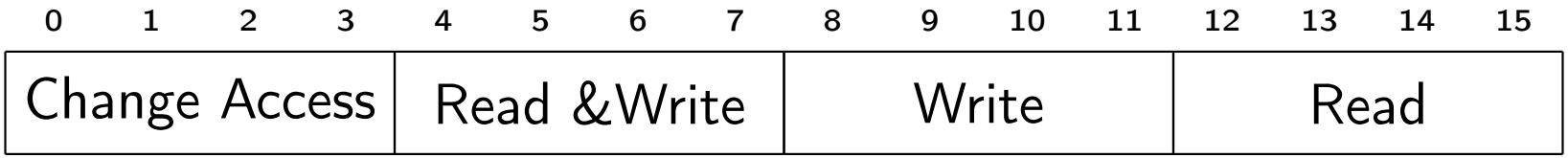
AID 0

- „Die Karte“
- Keine Dateien
- Nur ein Schlüssel: PICC Master Key
- Karte löschen, Applikationen erstellen/löschen, Einstellungen ändern, Karte einfrieren

Rest

- Bis zu 14 Schlüssel
- Schlüsselid 0: Application Master Key (AMK)
- Beliebige Kombinationen von Berechtigungen auf Schlüssel

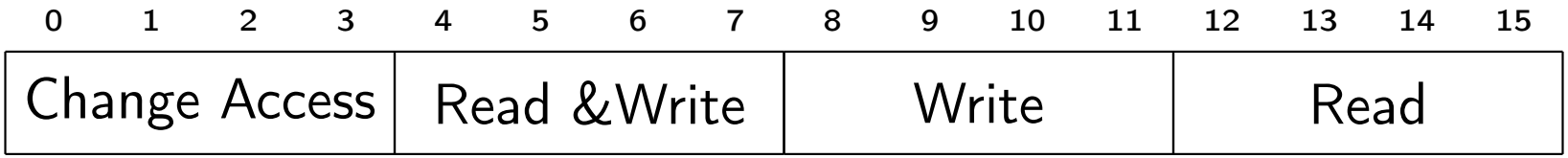
Dateiberechtigungen



Magische Schlüssel

- E Jeder
- F Keiner

Dateiberechtigungen



Magische Schlüssel

E	Jeder
F	Keiner

Value files

Read	GetValue, Debit
Write	LimitedCredit + Read
Read&Write	Credit + Write

Kommunikationsmodus

Modi

0. Plain
1. MACed
3. Crypted

Kommunikationsmodus

Modi

- 0 Plain
- 1 MACed
- 3 Crypted

Achtung

Wenn eine relevante Zugriffsberechtigung `E` ist $\Rightarrow$ Plain

Kommunikationsmodus

Modi

0 Plain

1 MACed

3 Crypted

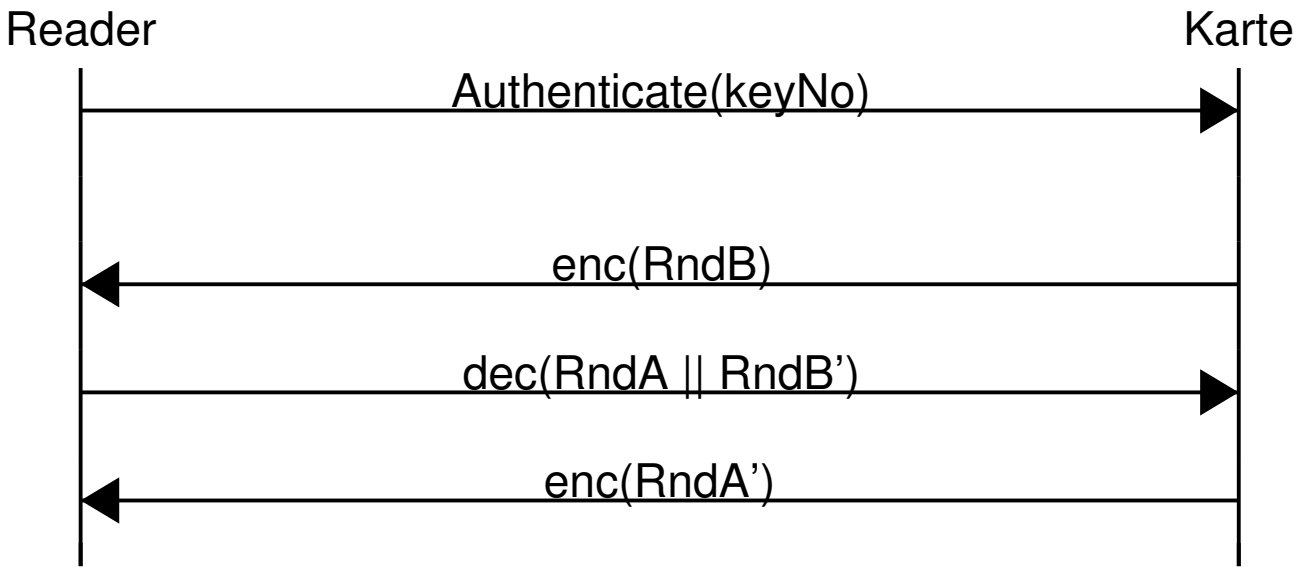
Achtung

Wenn eine relevante Zugriffsberechtigung `E` ist $\Rightarrow$ Plain

Crypted

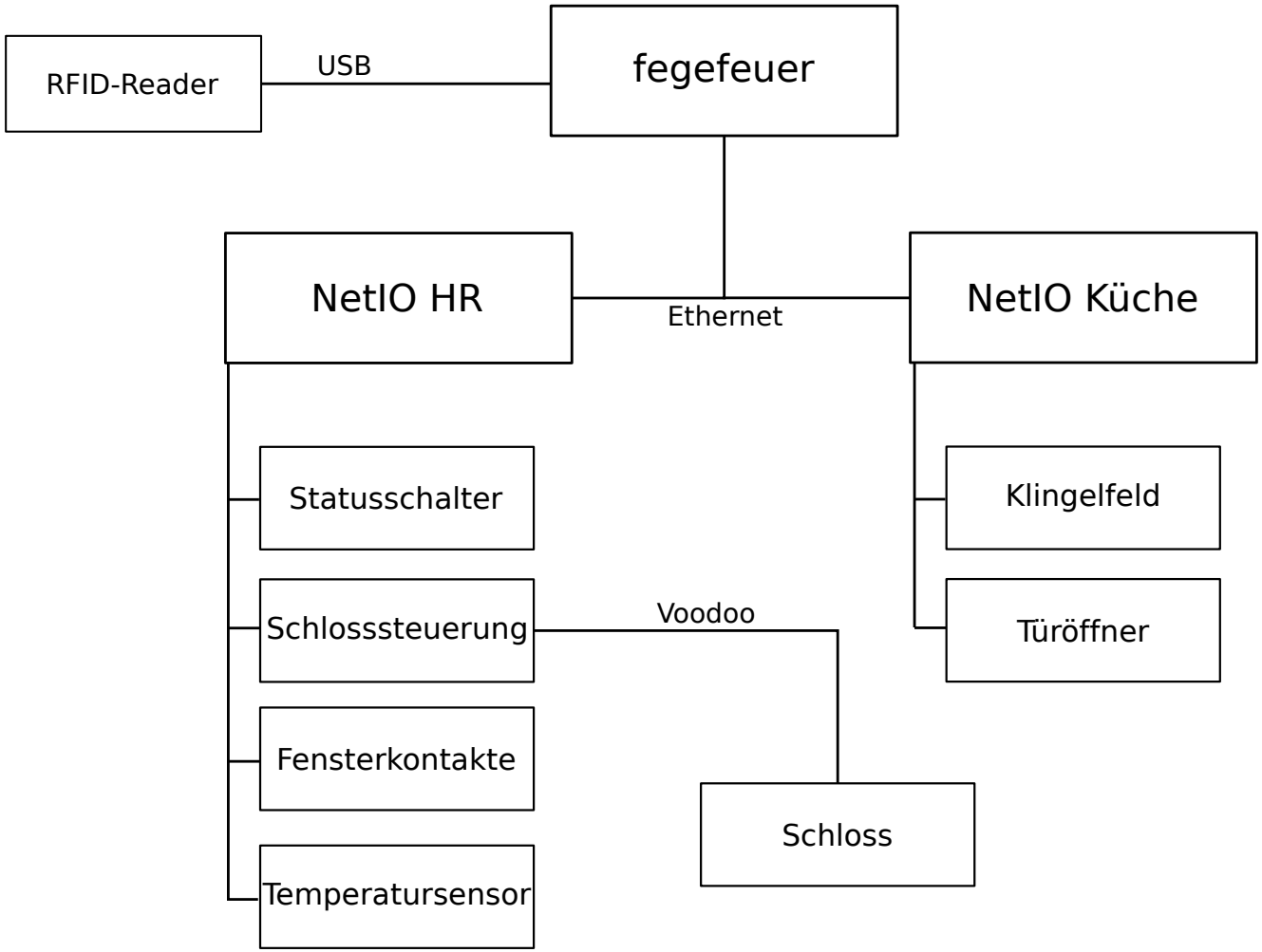
- CRC16 anhängen, DES mit CBC
- IV immer 0000000000000000

Authentifikation

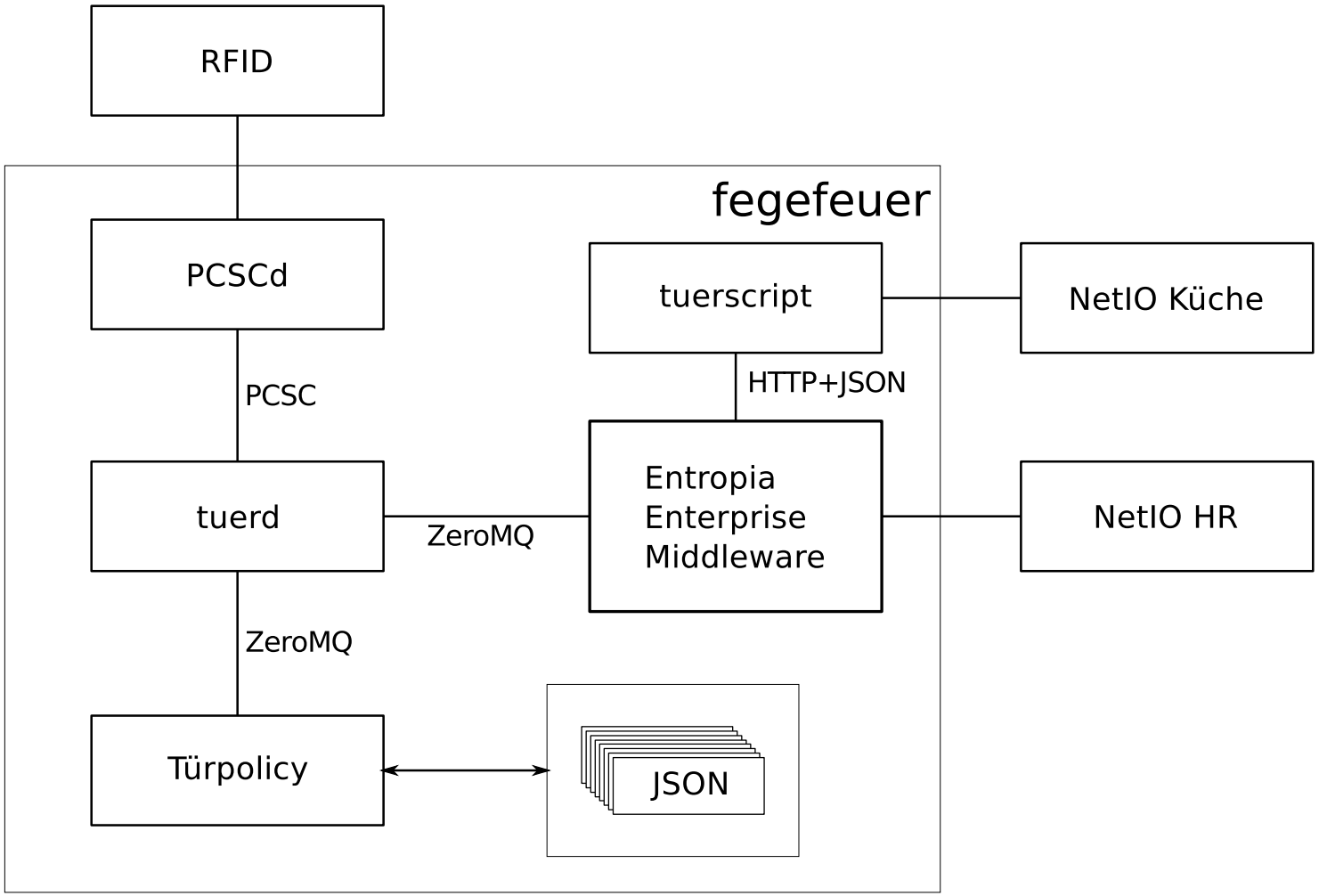


$$RndX' = rol(RndX, 8)$$
$$sk = RndA1||RndB1||RndA2||RndB2$$

Hardware


RFID-Reader
USB
fegefeuer
NetIO HR
Ethernet
NetIO Küche
Statusschalter
Klingelfeld
Schlosssteuerung
Voodoo
Türöffner
Fensterkontakte
Schloss
Temperatursensor

Software


RFID
fegefeuer
PCSCd
tuerscript
NetIO Küche
PCSC
HTTP+JSON
tuerd
ZeroMQ
Entropia
Enterprise
Middleware
NetIO HR
ZeroMQ
Türpolicy
JSON

JSON

```
{
    "user": "florolf",
    "buergen": ["foo", "bar", "qux"],
    "card": {
        "uid": "00010203040506",
        "picc_key": "6997FA088A3E9079B609B85CC81844C5",
        "ca0523_amk": "13F64D4F452FEBB56010F8A981CC82FB",
        "ca0523_door_key": "D7001CF78B91CBEF6350EB25832E17F3"
    }
}
```

Tür

Daten auf der Karte

- Applikation: `0xCA0523`
- Schlüssel `0xD` (shared secret mit der Tür)

1. *GetVersion*() $\rightarrow$ UID
2. Schlüssel nachschlagen
3. *SelectApplication*(`0xCA0523`)
4. *Authenticate*(`0xD`)

Und weiter?

- Getränkekasse
- Bessere Kryptographie (z.B. kontaktlose JavaCards)
- Selber rumspielen

Fragen?