

# Sicherheit/Datenschutz

## FH Schmalkalden setzt auf sichere Chipkarte

Die FH Schmalkalden hat sich für den Einsatz einer sicheren Chipkartentechnologie für den Studierendenausweis *thoska* entschieden. Anstelle des in negative Schlagzeilen gekommenen RFID-Chip "Mifare Classic" wird jetzt der sogenannte "Mifare DESFire" Chip in Verbindung mit der *thoska* eingesetzt werden. Der Mifare DESFire Chip ist mit einem eigenen Prozessor ausgestattet und daher in der Lage, deutlich höhere Sicherheitsanforderungen zu bewältigen. Das Verschlüsselungsverfahren des Mifare DESFire Chips basiert auf dem bewährten "Data Encryption Standard" und wird auf dem Kartenchip bei jeder Nutzung dreimal mit drei unterschiedlichen Schlüsseln ("Triple-DES") angewendet. Gegenüber dem Mifare Classic Chip erhöht sich die Schlüssellänge damit von 48 Bit auf 168 Bit.

### Datenspeicherung

Die Datenspeicherung beschränkt sich auf folgende Daten:

- Matrikelnummer
- Bibliotheksbenutzernummer
- Kartenummer
- Status als Student
- Gültigkeit
- ggf. Aufladebetrag

### Okay vom Landesdatenschutzbeauftragten

Der Thüringer Landesbeauftragte für Datenschutz hat sich nicht gegen den Einsatz der *thoska* ausgesprochen, wie in seinem 7. Tätigkeitsbericht auf Seite 101 nachzulesen ist.

<http://www.thueringen.de/datenschutz> - [Tätigkeitsbericht](#)

### Betrachtung der RFID-Technologie

- **RFID** = **R**adio **F**requently **I**Dentification - Identifizierung mit Hilfe von elektromagnetischen Wellen
- unter RFID versteht man Methoden, um Daten auf einem Transponder berührungslos und ohne Sichtkontakt lesen und schreiben zu können
- die 2 Komponenten eines RFID-Systems:
  - Transponder (Datenträger, Radiofrequenzmodul sendet und empfängt Daten - aktiv oder passiv)
  - Lesegerät (Schreib-/Leseinheit, Antenne) kommuniziert mit Transponder

### Mifare:

- Mifare = Mikron Fare System, also Mikron Fahrgeld-System
- Mifare wurde zwischen 1990 und 1995 von der "Mikron Gesellschaft für integrierte Mikroelektronik" in Österreich entwickelt
- 1995 wurde Mikron GmbH von Phillips Semiconductors aufgekauft
- 2006 wurde Philips Semiconductors von Phillips abgetrennt als NXP Semiconductors
- Mifare-Technik wurde an einige andere Firmen lizenziert: z.B. Infineon, Atmel, Hitachi
- Mifare-Produktfamilie umfaßt eine große Anzahl verschiedener Chips mit unterschiedlichen Verschlüsselungstechniken und Speichergrößen

### Mifare Classic:

- Mifare Classic wird als Oberbegriff für die Teilfamilie verwendet, die nur das alte Crypto-1-Verfahren als Verschlüsselungsalgorithmus und daher mehr oder weniger direkt von den ursprünglichen Mifare-Chips abgeleitet sind. Die verschiedenen Varianten des Chips haben wegen ihres guten Preis/Leistungsverhältnisses weltweit den größten Marktanteil bei kontaktlosen Speicherkarten mit Sicherheitsfunktionen
- Der Algorithmus konnte von Forschern des Chaos Computer Club und der University of Virginia entschlüsselt werden.
- Wie am 13. April 2008 bekannt wurde, hat eine Forschergruppe den Algorithmus analysiert und einen systematischen Fehler gefunden, der die Verschlüsselung praktisch nutzlos macht. Die Sicherheit des Algorithmus, so das Fazit der Forscher, sei "nahe Null".

### Mifare DESFire:

- ist eine Mikroprozessorkarte mit fest vorgegeben Betriebssystem im ROM
- Hauptmerkmal ist die Triple-**DES**-Verschlüsselung (dreifache Verschlüsselung mit mindest. 3 unterschiedlichen Schlüsseln)
- etwas teurere, aber sichere und flexible Alternative zu Mifare Classic
- unterstützt bis zu 28 Applikationen mit 16 Files pro Applikation
- mit einer Transferrate von 424 kBit/s ist er recht schnell und für die Verarbeitung umfangreicher Prozesse geeignet.
- passiver Transponder
- Funkfrequenz: 13,56 MHz
- Funkreichweite: bis zu 10 cm
- wird auch in der NASA in der Zugangskarte der Mitarbeiter eingesetzt
- Philips über Mifare DESFire:  
Mifare DESFire von Philips ist eine benutzerfreundliche multifunktionale Smart Card-Chiplösung, die sich ideal für mobile, Identifikations- und e-Government-Systeme eignet. Die Haupteigenschaften des Chips - "**F**ast, **I**nnovative, **R**eliable und **sE**cure", kurz "**Fire**" - werden durch eine flexible Speicherorganisation und hohe Datenübertragungsraten ergänzt. Daher eignet sich Mifare DESFire optimal für sichere kontaktlose Anwendungen.