

# Smartcard-Schnittstelle nach ISO/IEC 7816

Betreuung: Michael Roland

Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile)

## Motivation

Beim der Implementierung von Smartcard-Lesesoftware ist es unumgänglich die Protokollabläufe automatisiert zu testen. Während positive Testfälle, d.h. jene Fälle in denen die Lesesoftware gültige Eingabewerte bekommt, mit regulären Smartcards abgedeckt werden können, sind negative Testfälle nur schwer modellierbar. Viele Implementierungen von Smartcard-APIs (z.B. Java Smartcard IO und Windows PC/SC) bieten daher die Möglichkeit virtuelle Smartcard-Lesegeräte zu implementieren um so die von der Lesesoftware gesendeten Befehle in Testapplikationen umzuleiten. Möchte man jedoch ganze Lesegerätsysteme (d.h. die Lesesoftware in Kombination mit der Lesehardware) testen, dann ist dazu eine Hardware notwendig, welche die Schnittstelle einer Smartcard (ISO/IEC 7816) emuliert und so das Lesegerät an eine Testapplikation anbindet.

## Aufgabenstellung

Ziel dieser Arbeit ist es, einen solchen Smartcard-Emulator zu implementieren. Auf der einen Seite soll dieser Emulator mit einem Smartcard-Lesegerät über die standardisierten Smartcard-Protokolle (T=0 bzw. T=1 nach ISO/IEC 7816-3) kommunizieren. Am anderen Ende soll der Emulator die Datenpakete des Applikationsprotokolls (APDU, Application Protocol Data Unit) an eine PC-Applikation weiterleiten (z.B. über USB bzw. eine serielle Schnittstelle). Nach der Verarbeitung durch die PC-Applikation sollen die Antwortpakete über den Emulator zurück an das Lesegerät gesendet werden. Eventuell kann bei Teilen der Implementierung auf Ar-

beiten von Choudary [1] sowie de Koning Gans und de Ruiter [3] zurückgegriffen werden.

Nachdem das Testen der Implementierungen von Applikationsprotokollen im Vordergrund steht ist es ausreichend auf der Ebene von APDUs zu arbeiten. Die Manipulation von Parametern der unteren Protokollebenen (z.B. Framing, Timing) ist in der ersten Version des Emulators nicht notwendig.

## Ziele

- >> Auseinandersetzung mit ISO/IEC 7816 Smartcard-Protokollen (T=0, T=1, APDUs)
- >> Analyse der Anforderungen an einen Smartcard-Emulator
- >> Implementierung eines Smartcard-Emulators zum Austausch von Befehlen zwischen einem PC und einem Lesegerät über die ISO/IEC 7816 Schnittstelle
- >> Testweise Emulation einer Smartcard mittels PC-Programm

## Literatur

- [1] Choudary, O.S.: The Smart Card Detective: a handheld EMV interceptor. Master's thesis, University of Cambridge (Jun 2010)
- [2] ISO/IEC 7816: Identification cards – Integrated circuit(s) cards with contacts
- [3] de Koning Gans, G., de Ruiter, J.: The SmartLogic Tool: Analysing and Testing Smart Card Protocols. In: ICST 2012. pp. 864–871 (Apr 2012)
- [4] Rankl, W., Effing, W.: Handbuch der Chipkarten. Hanser München, 5th edn. (2008)

## Themenfelder

- >> Chipkarten
- >> Embedded Systeme
- >> Hardware, Software

## Kontakt

Dr. Michael Roland  
+43 (0)50804-27149  
michael.roland@fh-hagenberg.at

