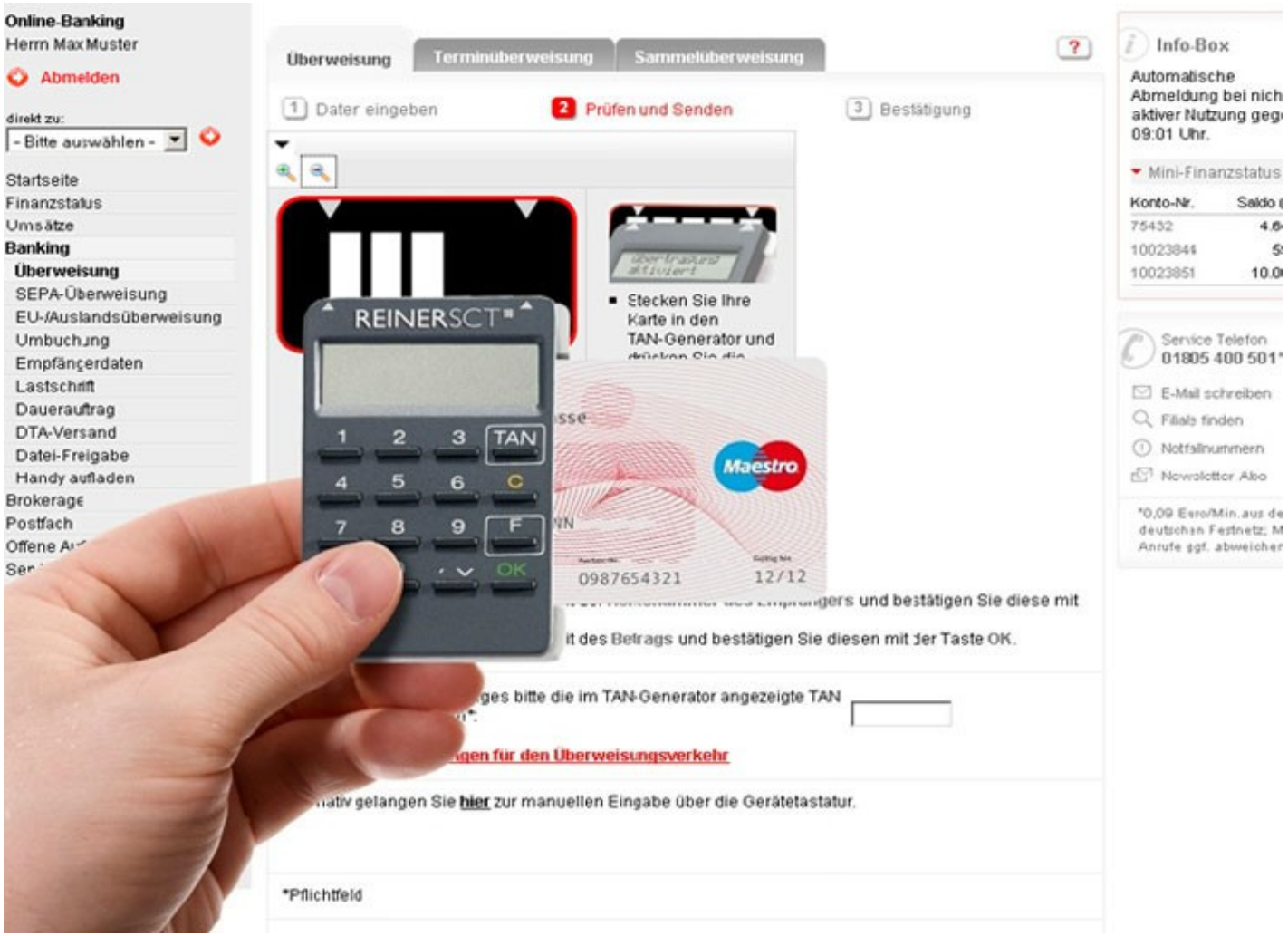
Analyse Kommunikation ChipTan

IT-Security Workshop
17.9 – 28.9

Kai Warncke, Michel Manthey, David Salomon

ChipTan Verfahren



Flickercode

Werkzeuge

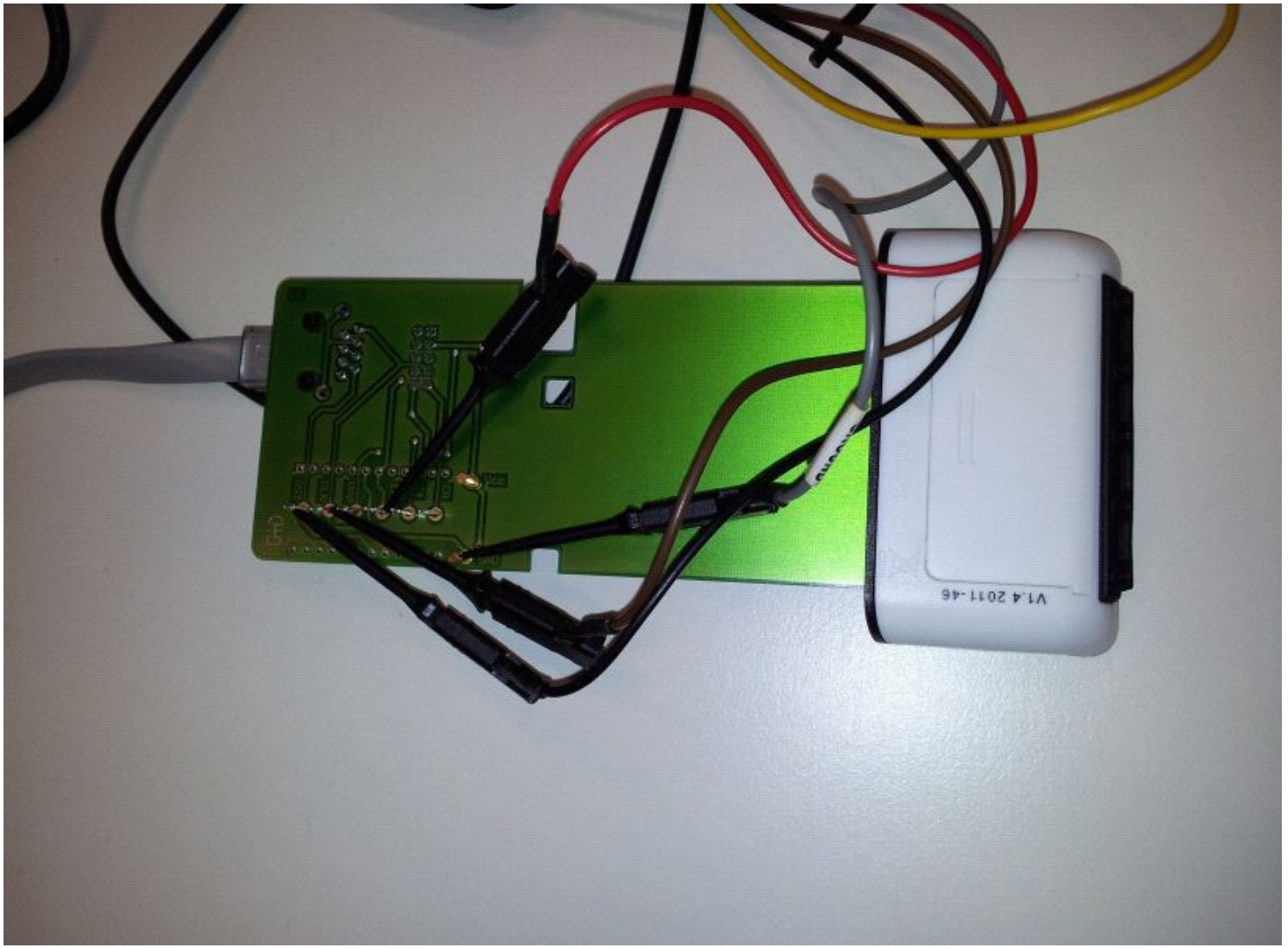
Saleae Logic Analyzer

Logic Software 1.1.15

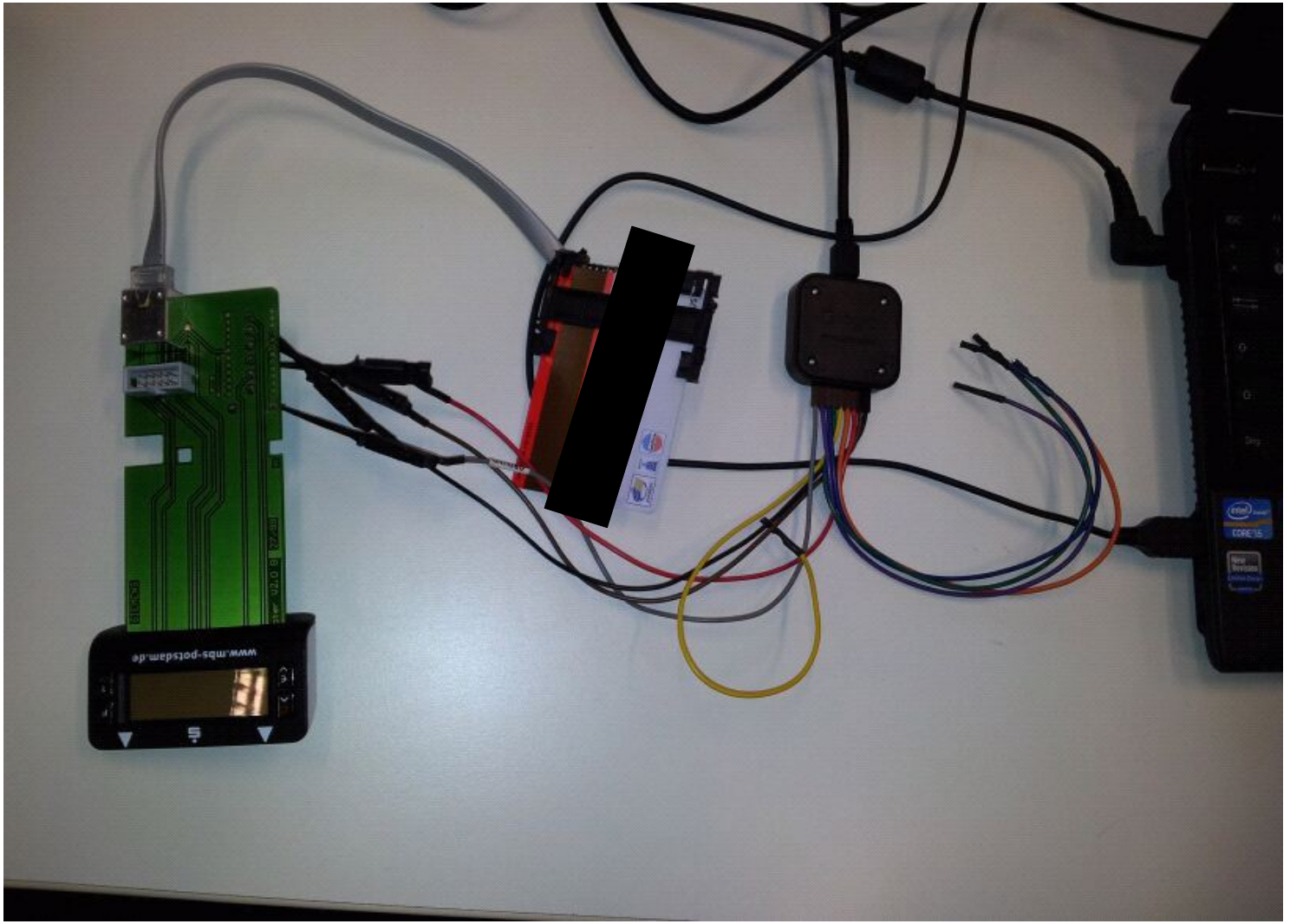
dazugehörige SDK (Software Development Kit)

Sparkassen Karte & Tan Generator

Versuchsaufbau

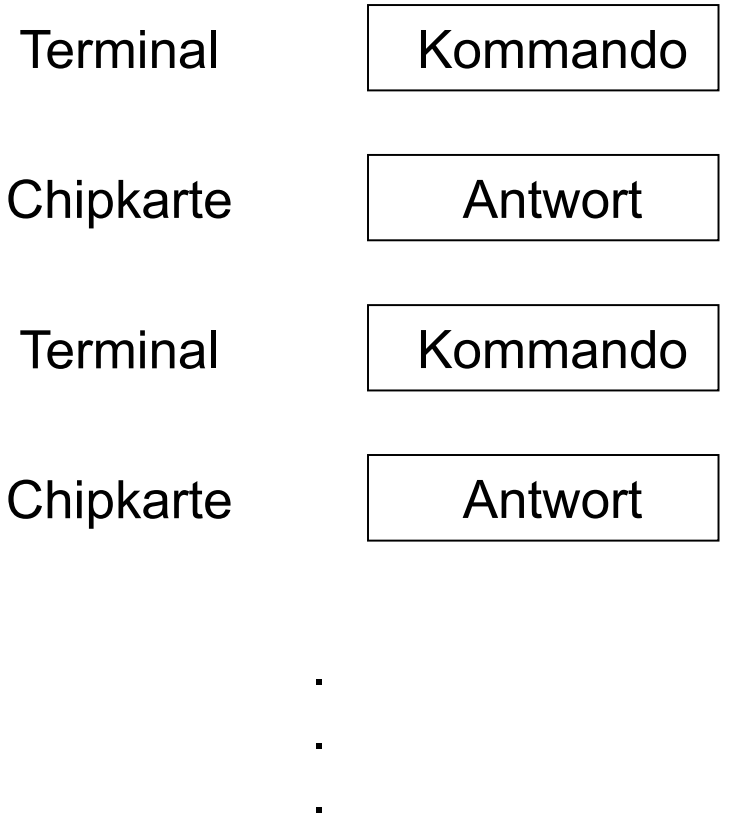


Versuchsaufbau



Michels Part

Kommunikationsablauf



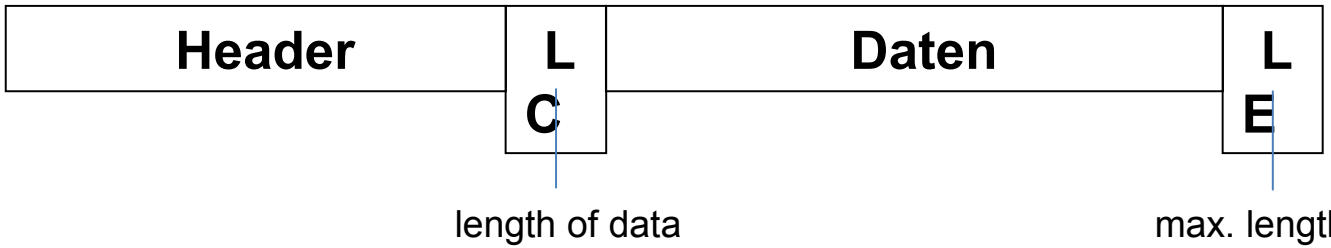
Kommando-Struktur

Prologfeld			Informationsfeld	Epilog
Knotenadresse NAD	Protokollkontrolbyte PCB	Länge LEN	APDU-Kommando	EDC
1 Byte	1 Byte	1 Byte	0 … 254 Byte	1 … 2 Byte

Block

Übertragungsprotokoll
T=1

APDU-Kommando



Case 1	Class	Instr	P1	P2		
Case 2	Class	Instr	P1	P2	LE	
Case 3	Class	Instr	P1	P2	LC	Daten
Case 4	Class	Instr	P1	P2	LC	Daten LE

Befehle

- SELECT Ordner, File oder Applikation
- READ RECORD
- SEARCH RECORD
- VERIFY
- PERFORM SECURITY OPERATION
- Kartenspezielle Befehle
- …

Test-Überweisung

T: S-Block: Systemänderung -> 254 Byte Info

C: Bestätigung

T: SELECT TAN Anwendung DF_TAN

C: Bestätigung

T: GET PROCESSING OPTIONS neue Transaktion

C: API und AFL

T: READ RECORD Kartendaten einlesen

C: Antwort Institut, Kartennr., Datum, Ländercode etc.

T: SEARCH RECORD IPB (issuer proprietary bitmap)

C: Antwort IPB (für TAN-Generierung wichtig)

…

Test-Überweisung

…

T: SEARCH RECORD (Daten für GENERATE AC)

C: Antwort

T: VERIFY

C: Bestätigung

T: HASH (Zielkonto und Betrag)

C: Antwort Hash/Wert

T: GENERATE AC mit Hash-Wert

C: Antwort (cid, ATC, AC, IAD)

Ableitung der TAN

- GENERATE_AC-Antworten und Bitfilter IPB werden verundet
- Stellen wo IPB 1 ist, bleiben erhalten
- left-rotate 8: die 8 linkesten Bit kommen nach ganz rechts
- Umrechnung in Dezimalzahl -> TAN

Ausblick

Fehlerfälle testen (falsche Karten,...)

Tan Berechnung: ExportFile

Software Tan Generator

DANKE

Quellen

Wolfgang Rankl, Wolfgang Effing(2008 & 2012). Handbuch der Chipkarten. Carl Hanser Verlag München

https://wiki.ccc-ffm.de/projekte:tangenerator:start

http://6xq.net/blog/2010/flickercodes/