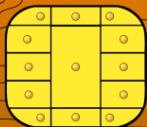


DIRECT

ID

PostFinance



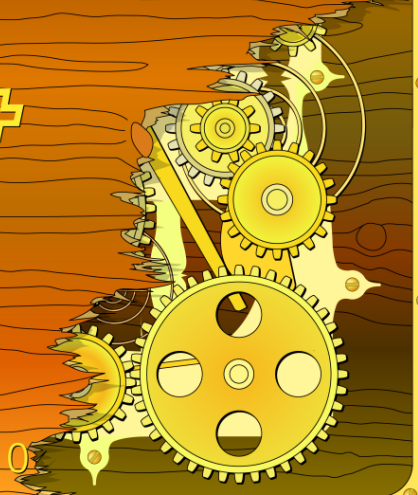
SWISS POST 

25132756

FREDDY TRAVOLTA

60-134597-1

0



Outline

- 1 Introduction
 - Recap of last years lecture about the swiss Postcard
 - This talk is about
 - What is a smartcard?
 - Everyone can build its own
- 2 Logging the communication
 - Hardware-based logging
 - RFID Relay / Logging Agent
 - Software-based logging
 - Comparison between methods
- 3 Re-engineering the protocol
 - Principle of communication logging
 - Hands on example
 - Data structure for a logging application
- 4 Creating a simulacrum

Outline

- 1 Introduction
 - Recap of last years lecture about the swiss Postcard
 - This talk is about
 - What is a smartcard?
 - Everyone can build its own
- 2 Logging the communication
 - Hardware-based logging
 - RFID Relay / Logging Agent
 - Software-based logging
 - Comparison between methods
- 3 Re-engineering the protocol
 - Principle of communication logging
 - Hands on example
 - Data structure for a logging application
- 4 Creating a simulacrum

Recap of last years lecture about the swiss Postcard I

- 1979 Start design of PIN protected memory card (Bull CP8)
- 1983 French banking card with 320 bit RSA authentication
- 1989 Introduction of french banking card (*Carte Bleue*)
- 1998 **Serge Humpich** re-engineered the *Carte Bleue*

Recap of last years lecture about the swiss Postcard II

- 2002 Found that the security measures of the *swiss Postcard* were similar
- 2006 Re-checked the security measures
- 2006 Presentation of initial results at the 23C3:
A not so smart card
- 2007 initiated academic response
eg. <http://lis.fh-aargau.ch/ecsem/ECSeminar/SS07.html>
 - low impact, small media coverage

This talk is about

- **PostFinance**

Flawed signatures not used in authentication scheme

- **Goal**

Build a working Postcard clone based on known facts

- For an introduction into the design flaws take a look at *postcard-sicherheit.ch*

This talk is about

- **PostFinance**

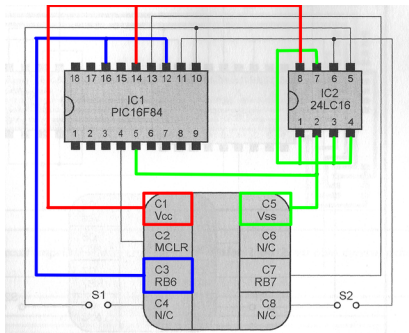
Flawed signatures not used in authentication scheme

- **Goal**

Build a working Postcard clone based on known facts

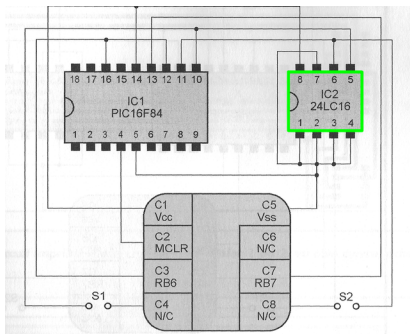
- For an introduction into the design flaws take a look at *postcard-sicherheit.ch*

What is a smartcard?



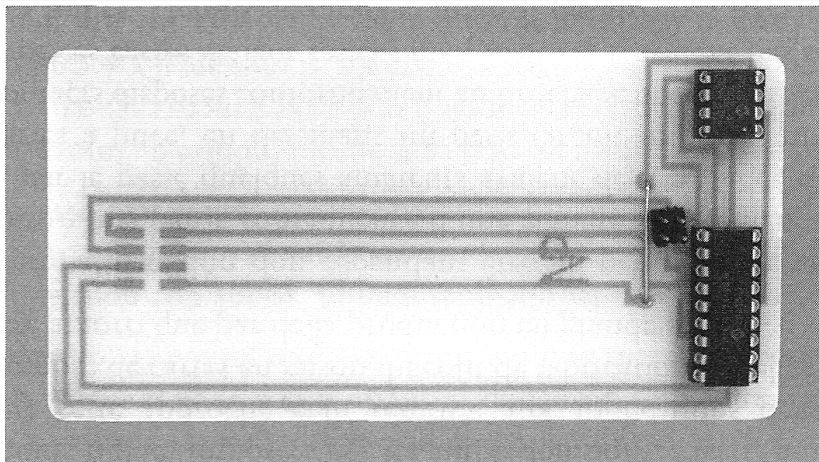
- External clock, ground and energy source
- I/O (input - output), reset
- Microcontroller with an internal EEPROM
- External EEPROM

What is a smartcard?



- External clock, ground and energy source
- I/O (input - output), reset
- Microcontroller with an internal EEPROM
- External **EEPROM**

Everyone can build its own



Comparable to an old 8bit PC (but with fewer passive elements).

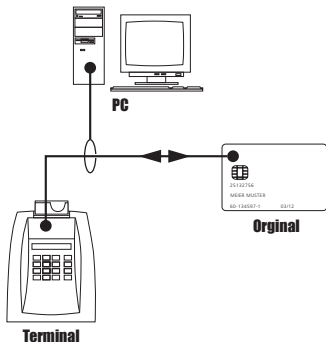
Outline

- 1 Introduction
 - Recap of last years lecture about the swiss Postcard
 - This talk is about
 - What is a smartcard?
 - Everyone can build its own
- 2 Logging the communication
 - Hardware-based logging
 - RFID Relay / Logging Agent
 - Software-based logging
 - Comparison between methods
- 3 Re-engineering the protocol
 - Principle of communication logging
 - Hands on example
 - Data structure for a logging application
- 4 Creating a simulacrum

Protocol is mostly known

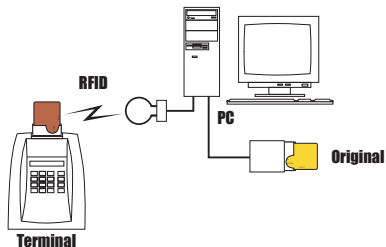
- Most cards use ISO-7816 protocol to communicate with terminal
- ISO-7816 defines all aspects (physical/logical specs)
- Compatibility leads to tolerance (timing less relevant if within range)
- Still necessary even if protocol is published (like EMV) ?

Hardware-based logging



- Pro** Capture the communication on physical level (timing)
- Con** Not feasible outdoors

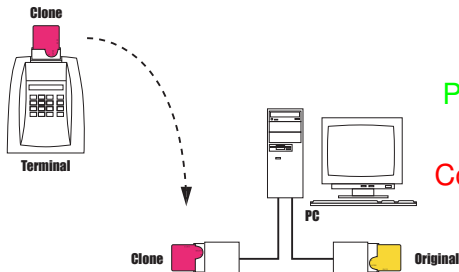
RFID Relay / Logging Agent



- Pro** Full processing power and comfort
- Con** No known implementation yet

Communicate with inserted card via RFID form notebook.

Software-based logging



- Pro** (Quite) easy to program and use (secrecy)
- Con** Step-by-step approach (time consuming)

Use programmable smartcards to capture communication.

Javacard / Processorcard

Javacard

- Pro** No special programmer needed
- Con** Can't log *direct convention* or T1

Processorcard

- Pro** Can be customized to any sort of communication
- Con** Needs special programmer (Money)

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Comparison between methods

Property	HW	JC	PC
Capture timing	X		
T1 protocol	X		X
Direct convention	X		X
Indirect convention	X	X	X
Ease of use	lo	hi	med*
Secrecy	lo	hi	hi
Special hardware	X		X

*Increase with ISO-7816/T0 library

Outline

- 1 Introduction
 - Recap of last years lecture about the swiss Postcard
 - This talk is about
 - What is a smartcard?
 - Everyone can build its own
- 2 Logging the communication
 - Hardware-based logging
 - RFID Relay / Logging Agent
 - Software-based logging
 - Comparison between methods
- 3 Re-engineering the protocol
 - Principle of communication logging
 - Hands on example
 - Data structure for a logging application
- 4 Creating a simulacrum

Principle of communication logging

Terminal

Logger

Smartcard

request



Lookup in
request list



Found: Send
associated response



Unknown: Send *ok*
Start logging

repeat

Replay



Save



response

restart

Principle of communication logging

Terminal

Logger

Smartcard

request



Lookup in
request list



Found: Send
associated response



Unknown: Send *ok*
Start logging

repeat

Replay



Save



response

restart

Principle of communication logging

Terminal

Logger

Smartcard

request



Lookup in
request list



Found: Send
associated response



Unknown: Send *ok*
Start logging

repeat

Replay



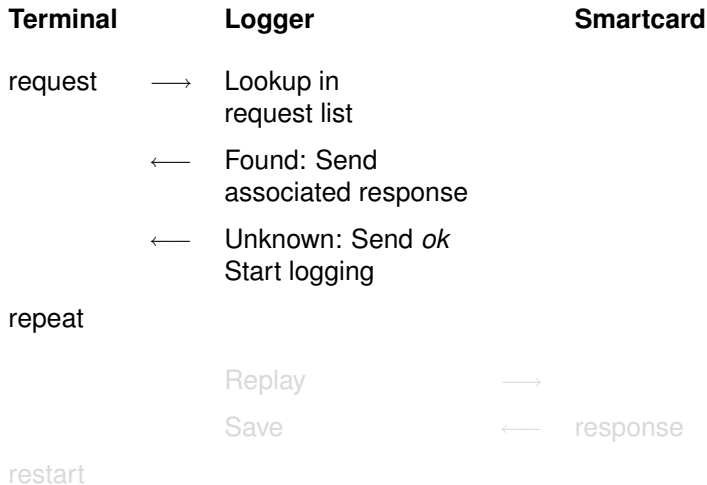
Save



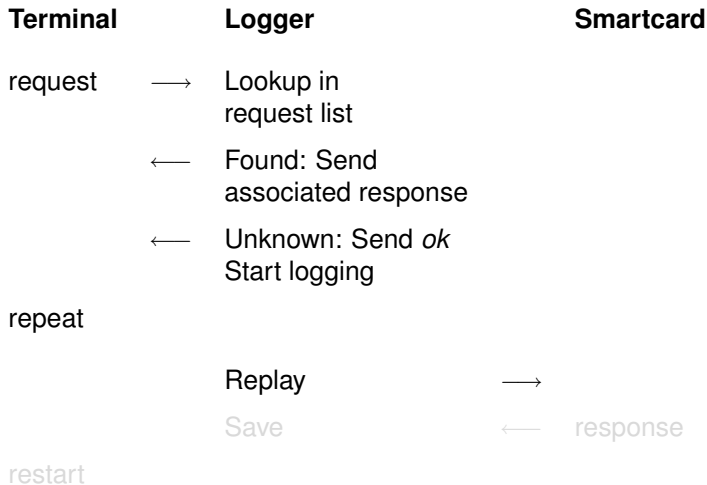
response

restart

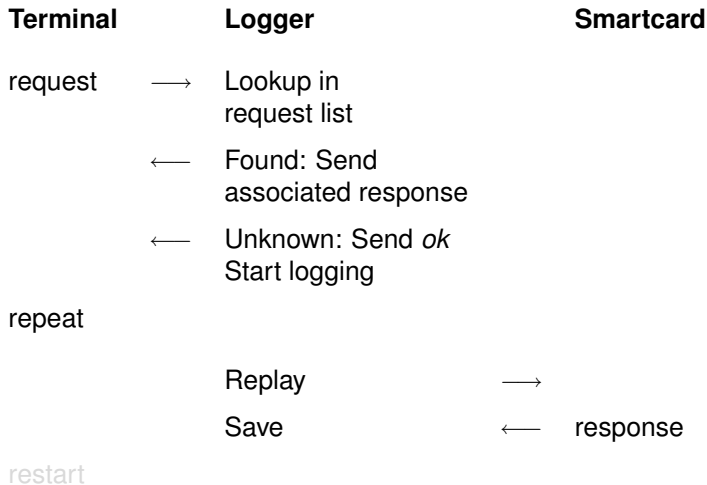
Principle of communication logging



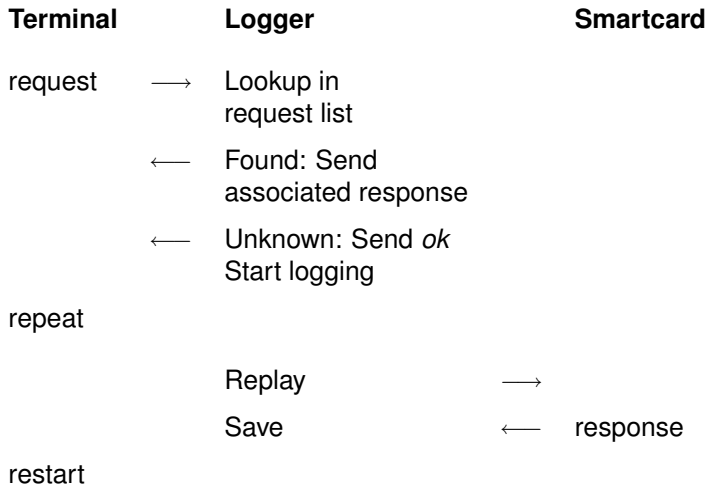
Principle of communication logging



Principle of communication logging



Principle of communication logging



Communication

Terminal

(Power on)
BC:B0:09:C0:1C
BC:B0:09:F8:04
BC:B0:08:E0:1C
BC:B0:09:18:1C

BC:B0:08:B0:04 [6A81]
BC:20:00:00:04:XX:XX:XX:XX [9000]
BC:40:00:00:00 [9000]
BC:B0:08:B0:04

Smartcard

3B:65:00:00:02:04:6C:90:00
08:4D:FF:FF:23:9F:0B:EB:... [9000]
3E:AC:9F:CC [9000]
2E:03:30:33:3X:XX:XX:XX:... [9000]
3X:XX:XX:XX:3X:XX:XX:XX:... [9000]

[6A81]
[9000]
[9000]
75:XX:XX:XX [9000]

Sending the ATR

Terminal

(Power on)

Smartcard

ATR - Answer To Reset
3F:65:35:10:02:04:6C:90:00

TS Initial Character 3F: indirect convention

T0 Format Character 65: TB1, TC1 and 5 historicals

TB1 35 Programming voltage 5.3 V

TC1 10 Extra guardtime $10 * 104 \mu s$

HS Historicals

Sending the ATR

Terminal

(Power on)

Smartcard

ATR - Answer To Reset

3F:65:35:10:02:04:6C:90:00

TS Initial Character **3F**: indirect convention

T0 Format Character **65**: TB1, TC1 and 5 historicals

TB1 **35** Programming voltage 5.3 V

TC1 **10** Extra guardtime $10 * 104 \mu\text{s}$

HS Historicals

Sending the ATR

Terminal

(Power on)

Smartcard

ATR - Answer To Reset

3F:65:35:10:02:04:6C:90:00

TS Initial Character **3F**: indirect convention

T0 Format Character **65**: TB1, TC1 and 5 historicals

TB1 **35** Programming voltage 5.3 V

TC1 **10** Extra guardtime $10 * 104 \mu\text{s}$

HS Historicals

Sending the ATR

Terminal

(Power on)

Smartcard

ATR - Answer To Reset

3F:65:35:10:02:04:6C:90:00

TS Initial Character 3F: indirect convention

T0 Format Character 65: TB1, TC1 and 5 historicals

TB1 35 Programming voltage 5.3 V

TC1 10 Extra guardtime $10 * 104 \mu s$

HS Historicals

Sending the ATR

Terminal

(Power on)

Smartcard

ATR - Answer To Reset

3F:65:35:10:02:04:6C:90:00

TS Initial Character 3F: indirect convention

T0 Format Character 65: TB1, TC1 and 5 historicals

TB1 35 Programming voltage 5.3 V

TC1 10 Extra guardtime $10 * 104 \mu s$

HS Historicals

Sending the APDU

Terminal

(Power on)
BC:B0:09:C0:1C

Smartcard

3B:65:00:00:02:04:6C:90:00

CLA BC Banking cards.

INS B0 Read data

ADDR at address 09:C0

LC and return 1C bytes.

* APDU - Application Protocol Data Unit.

Sending the APDU

Terminal

(Power on)

BC:B0:09:C0:1C

CLA BC Banking cards.

INS B0 Read data

ADDR at address 09:C0

LC and return 1C bytes.

* APDU - Application Protocol Data Unit.

Smartcard

3B:65:00:00:02:04:6C:90:00

Sending the APDU

Terminal

(Power on)

BC:B0:09:C0:1C

CLA BC Banking cards.

INS B0 Read data

ADDR at address 09:C0

LC and return 1C bytes.

* APDU - Application Protocol Data Unit.

Smartcard

3B:65:00:00:02:04:6C:90:00

Sending the APDU

Terminal

(Power on)

BC:B0:09:C0:1C

CLA BC Banking cards.

INS B0 Read data

ADDR at address 09:C0

LC and return 1C bytes.

* APDU - Application Protocol Data Unit.

Smartcard

3B:65:00:00:02:04:6C:90:00

Sending the APDU

Terminal

(Power on)

BC:B0:09:C0:1C

CLA BC Banking cards.

INS B0 Read data

ADDR at address 09:C0

LC and return 1C bytes.

* APDU - Application Protocol Data Unit.

Smartcard

3B:65:00:00:02:04:6C:90:00

Stateful lookup

Terminal

(Power on)

BC:B0:09:C0:1C

BC:B0:09:F8:04

BC:B0:08:E0:1C

BC:B0:09:18:1C

BC:B0:08:B0:04

BC:20:00:00:04:XX:XX:XX:XX [9000]

BC:40:00:00:00

BC:B0:08:B0:04

Smartcard

(ATR) 3B:65:00:00:02:04:6C:90:00

08:4D:FF:FF:23:9F:0B:EB:... [9000]

3E:AC:9F:CC [9000]

2E:03:30:33:3X:XX:XX:XX:... [9000]

3X:XX:XX:XX:3X:XX:XX:XX:... [9000]

[6A81]

[9000]

[9000]

75:XX:XX:XX [9000]

Stateful lookup

Terminal

(Power on)
BC:B0:09:C0:1C
BC:B0:09:F8:04
BC:B0:08:E0:1C
BC:B0:09:18:1C

BC:B0:08:B0:04
BC:20:00:00:04:XX:XX:XX:XX
BC:40:00:00:00
BC:B0:08:B0:04

Smartcard

(ATR) 3B:65:00:00:02:04:6C:90:00
08:4D:FF:FF:23:9F:0B:EB:... [9000]
3E:AC:9F:CC [9000]
2E:03:30:33:3X:XX:XX:XX:... [9000]
3X:XX:XX:XX:3X:XX:XX:XX:... [9000]

[6A81]
[9000]
[9000]
75:XX:XX:XX [9000]

Stateful lookup

Terminal

(Power on)
BC:B0:09:C0:1C
BC:B0:09:F8:04
BC:B0:08:E0:1C
BC:B0:09:18:1C

BC:B0:08:B0:04

BC:20:00:00:04:XX:XX:XX:XX [9000]

BC:40:00:00:00

BC:B0:08:B0:04

Smartcard

(ATR) 3B:65:00:00:02:04:6C:90:00
08:4D:FF:FF:23:9F:0B:EB:... [9000]
3E:AC:9F:CC [9000]
2E:03:30:33:3X:XX:XX:XX:... [9000]
3X:XX:XX:XX:3X:XX:XX:XX:... [9000]

[6A81]

75:XX:XX:XX [9000]

Stateful lookup

Terminal

(Power on)
BC:B0:09:C0:1C
BC:B0:09:F8:04
BC:B0:08:E0:1C
BC:B0:09:18:1C

BC:B0:08:B0:04

BC:20:00:00:04:XX:XX:XX:XX [9000]

BC:40:00:00:00

BC:B0:08:B0:04

Smartcard

(ATR) 3B:65:00:00:02:04:6C:90:00
08:4D:FF:FF:23:9F:0B:EB:... [9000]
3E:AC:9F:CC [9000]
2E:03:30:33:3X:XX:XX:XX:... [9000]
3X:XX:XX:XX:3X:XX:XX:XX:... [9000]

[6A81]

[9000]

[9000]

75:XX:XX:XX [9000]

Stateful lookup

Terminal

(Power on)
BC:B0:09:C0:1C
BC:B0:09:F8:04
BC:B0:08:E0:1C
BC:B0:09:18:1C

BC:B0:08:B0:04

BC:20:00:00:04:XX:XX:XX:XX [9000]

BC:40:00:00:00

BC:B0:08:B0:04

Smartcard

(ATR) 3B:65:00:00:02:04:6C:90:00
08:4D:FF:FF:23:9F:0B:EB:... [9000]
3E:AC:9F:CC [9000]
2E:03:30:33:3X:XX:XX:XX:... [9000]
3X:XX:XX:XX:3X:XX:XX:XX:... [9000]

[6A81]

[9000]

[9000]

75:XX:XX:XX [9000]

A data structure for a logging application - requests

Requests

offset	length	field
00	01	Index (0 = End)
01	01	Active State (0 = Any)
02	01	Next State (FF = no change)
03	01	Length of additional data (n)
04	05	APDU
09	n	<Additional data>

A data structure for a logging application - responses

Responses

offset	length	field
00	01	Index (0 = End)
01	01	Type (1 = SW, 2 = Data)
02	02	SW / Length (n)
04	n	<Data>

Treating the same card differently

Swisscom publicphone SBB ticket machine

BC:B0:09:C0:1C

BC:B0:09:F8:04

BC:B0:08:E0:1C

BC:B0:09:18:1C

BC:B0:09:50:1C

BC:B0:09:88:1C

BC:B0:09:C0:18

BC:B0:09:48:1C

Treating the same card differently

Swisscom publicphone SBB ticket machine

BC:B0:09:C0:1C

BC:B0:09:F8:04

BC:B0:08:E0:1C

BC:B0:09:18:1C

BC:B0:09:50:1C

BC:B0:09:88:1C

BC:B0:09:C0:18

BC:B0:09:48:1C

Outline

- 1 Introduction
 - Recap of last years lecture about the swiss Postcard
 - This talk is about
 - What is a smartcard?
 - Everyone can build its own
- 2 Logging the communication
 - Hardware-based logging
 - RFID Relay / Logging Agent
 - Software-based logging
 - Comparison between methods
- 3 Re-engineering the protocol
 - Principle of communication logging
 - Hands on example
 - Data structure for a logging application
- 4 **Creating a simulacrum**

Material you need

- **special reader**

<http://www.infinityusb.com>

Ask for better *Linux, BSD, Plan9, Solaris, OS/2* support!

- **avr-gcc**

<http://www.nongnu.org/avr-libc>

- **ISO-7816/T0 library**

<http://postcard-sicherheit.ch/de/clone.html>

Further information



postcard-sicherheit.ch

The ultimate source for *postcard* security.



parodie.com/monetique

Reference of the *Carte Bleue*.






mbsks.franken.de/sosse

Simple Operating System for Smartcard Education.



en.wikipedia.org/wiki/ISO_7816

Further reading

-  Rankl, Effing - Handbuch der Chipkarten
Reference.
-  Gueulle - Cartes à puce
Information about the french banking card.
-  Tavernier - Les cartes à puce
Hands on guide.

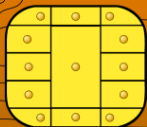
Questions?

Questions?

DIRECT

ID

PostFinance



SWISS POST 

25132756

FREDDY TRAVOLTA

60-134597-1

0

