A Not So Smart Card

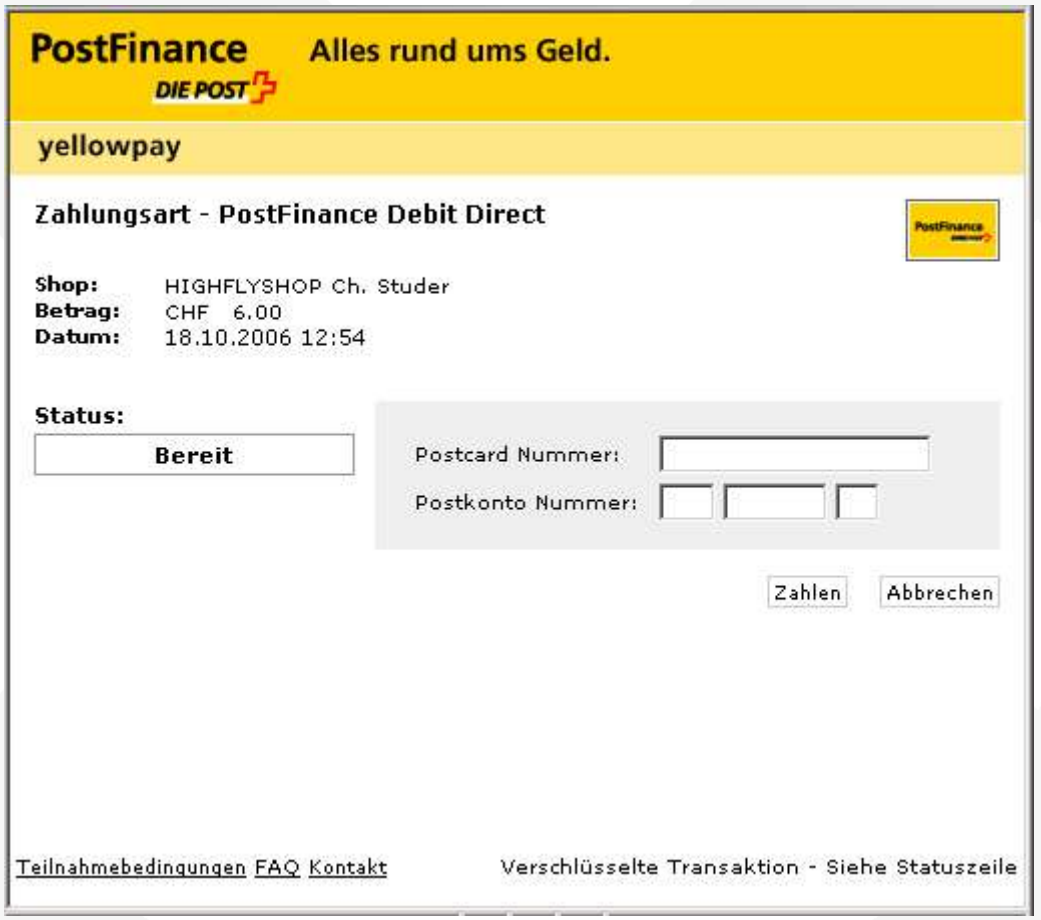
“Any sufficiently unadvanced technology requires a lot of magic …”

Bernd R. Fix <Bernd.Fix@aspector.com>

What we are talking about...

- ~ 2'500'000 users
- yearly figures:
  - ~ 700'000'000 transactions
  - ~ 8'000'000'000 Swiss Francs

“Secure” online transactions...



3F 65 35 10 02 04 6C 90 00 **ATR**

http://www.sun-rays.org/lib/smartcard_list.txt:

3F 65 25 .. .. 04 6C 90 00	**Carte Bancaire (french banking card)**
3F 65 25 00 22 09 F9 90 00	Sesam Vitale (french health card)
3F 65 25 00 2B 09 62 90 00	Coinamatic SmartyCity smartcard
3F 65 25 00 2B 09 EB 90 00	Bull Scot 5
3F 65 25 00 52 09 6A 90 00	French carte Vitale
3F 65 25 08 22 04 68 90 00	France Telecom card (ex Pastel card)
3F 65 25 08 33 04 20 90 00	D-Trust card
3F 65 35 64 02 04 6C 90 00	**Postcard (Switzerland)**

3F 65 35 10 02 04 6C 90 00	**ATR**	**3F 65 25 08 33 04 6C 90 00**
BC	**CLA**	**BC**
BC:B0:09:C8:02 ⇒ 23:9F	**ADL**	**BC:B0:09:C8:02 ⇒ 23:9F**

Converting ADL “pointer” to memory address:

239F

⇒ 0010 0011 1001 1111

⇒ 0010 0011 100 (000)

⇒ 00 1000 1110 0000

⇒ **08E0**

Reading memory content: BC:B0:08:E0:70

```
2E 03 30 33
30 00 04 55 32 E7 9E 84
3F A5 78 85 3X XX XX XX
3X XX XX XX 3X XX XX XX
3X XX XX XX 3X XX XX XX
3X XX XX XX 3X XX XX XX
3X XX XX XX 3X XX XX XX
2E 02 38 F1
30 05 01 62 3X XX XX XX
3X XX XX XX 3X 00 05 07
32 80 09 08 37 56 35 01
3Y YY YY YY 3Y YY YY YY
3Y YY YY YY 3Y YY YY YY
3Y YY Y2 02 30 20 20 20
32 02 02 02 30 20 F6 23
```

```
2E 03 30 33
30 00 03 90 37 83 46 D4
3A CC B5 E6 3X XX XX XX
3X XX XX XX 3X XX XX XX
3X XX XX XX 3X XX XX XX
3X XX XX XX 3X XX XX XX
3X XX XX XX 3X XX XX XX
2E 02 38 F1
30 04 97 XX 3X XX XX XX
3X XX XF FF 31 01 96 07
32 50 98 09 32 50 54 97
34 D5 22 0Y 3Y YY YY YY
3Y YY YY Y2 30 YY YY YY
3Y Y2 02 02 30 20 20 20
32 02 02 02 30 20 F0 20
```

- Analyzing the memory content
- Extracting the RSA modulus
- Factorizing the RSA modulus

If you are interested in the technical details:

Join the workshop at Day 3 (20:30 – 21:30)

A Not So Smart Card

Is this really

The End?

Bernd R. Fix <Bernd.Fix@aspector.com>