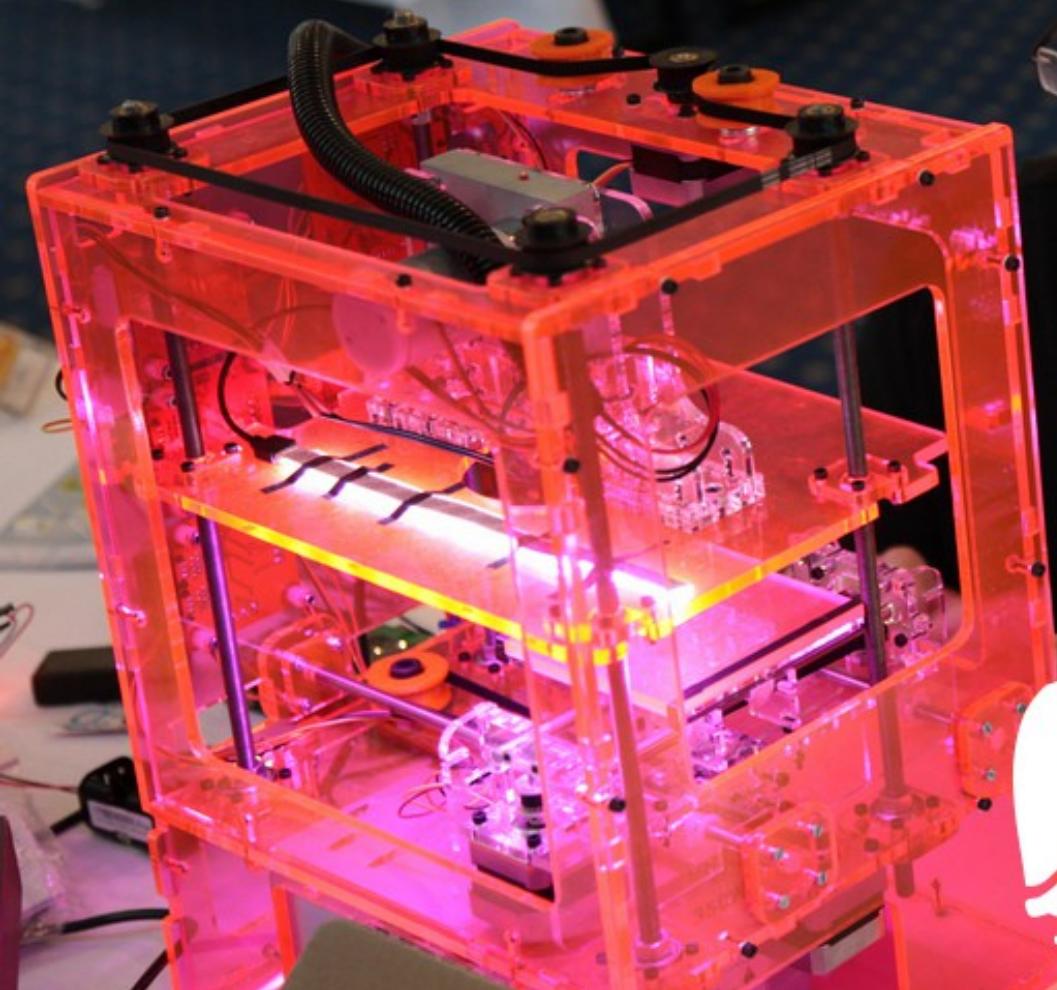






#	Avatar	Team	Location	Local	EC...	Ma...	Ge...	
1	More Smoked Leet Chicken	Russia	Yes	103	-	200		
2	Stratum Ruhuur	Germany	No	-	-	202		
3	PPP	United States	No	-	-	200		
4	Dragon Sector	Poland	No	-	-	200	200 150 400 150 - 253 400 500 402 - 200	
5	pollypocket	Belgium	Yes	-	-	200	202 150 402 150 203 - 250 400 500 400 - 200	
6	dcua	Ukraine	No	-	-	200	200 150 400 150 - 250 400 500 400 - 200	



OBSERVE

M1

- Authentication
- Challenge, then PIN, then response

M2

- Transaction signature
- PIN, then challenge*, then response

Digipass from bank A works with bank B

- So...

* denotes the zero-or-more regex operator



Ask big ~~friends~~ brothers



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001618 A2

(51) International Patent Classification⁷: **G06F**

Jean-Marie, Charles, Paic [BE/BE]. LASNES, Jean-Paul, Edmond, Rans [BE/BE]. NAMUR, Filret, Ates [BE/BE]. WANKMUELLER, John [US/US].

(21) International Application Number:
PCT/US2004/017756

(74) Agents: SCHEINFELD, Robert, C. et al.; Baker Botts LLP, 30 Rockefeller Plaza, New York, NY 10112-4498 (US).

(22) International Filing Date: 4 June 2004 (04.06.2004)

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(25) Filing Language: English

(75) Inventors; and

(26) Publication Language: English

(76) Priority Data:

60/475,639 4 June 2003 (04.06.2003) US

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

(71) Applicant (for all designated States except US): **MAS-TERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors; and

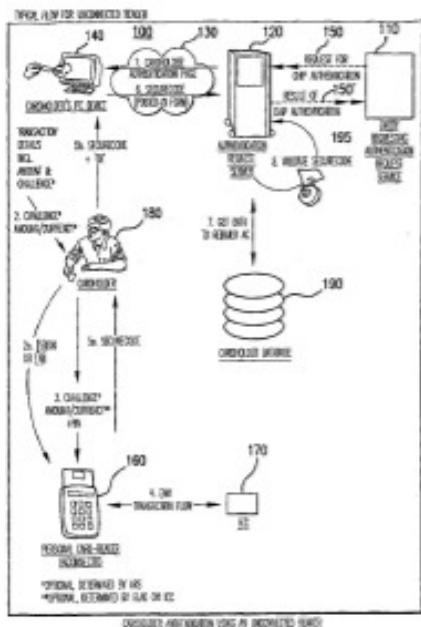
(73) Inventors/Applicants (for US only): **RUTHER-**

FORD, Bruce [US/US], **DAGHER, Alfred** [US/US],

WIESMAN, Mark [US/US], **RIXENSART, Didier**,

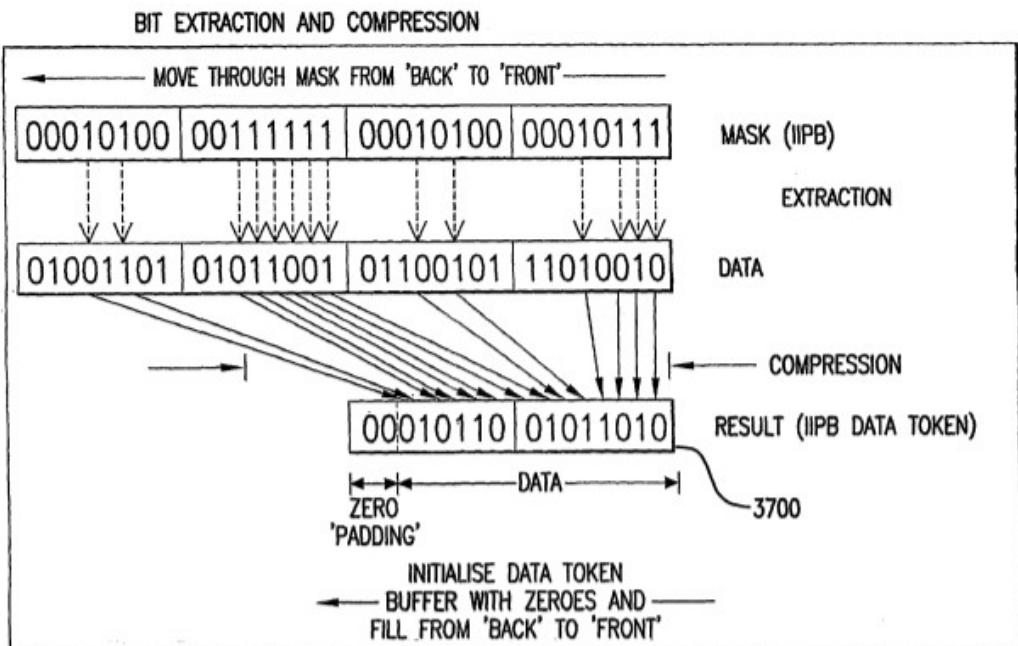
{Continued on next page}

(54) Title: CUSTOMER AUTHENTICATION IN E-COMMERCE TRANSACTIONS



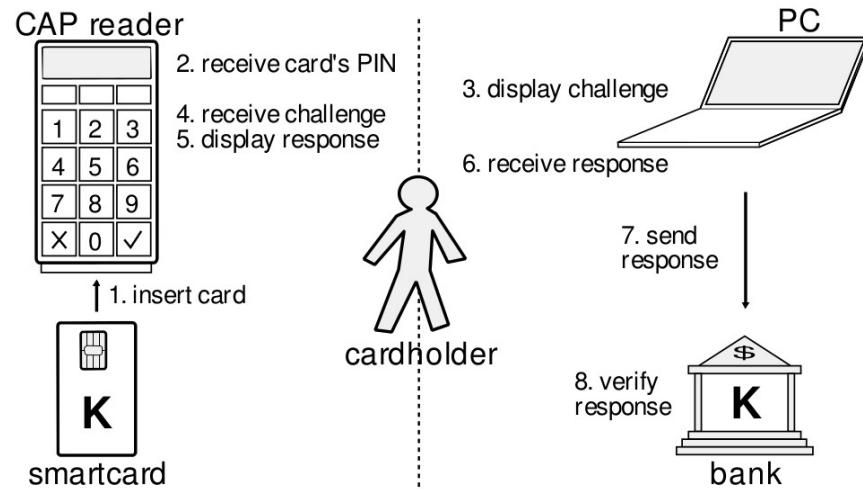
(57) Abstract: A Chip Authentication Program based on 3-D Secure protocols is provided for authenticating customers' on-line transactions. An issuer, who may be a payment card issuer, operates Access Control and Authentication Request Servers for authenticating transactions by individual customers who are identified by their personal EMV-compliant smart cards. An authentication token is generated at the point of interaction (POI) for each transaction based on information from the customer's smart card and transaction specific information sent directly by the issuer to populate a web page at the POI. Authentication tokens generated at the POI are evaluated by the Authentication Request Server to authenticate individual customer and/or card presence at the transaction POI. Authentication values are transported on-line in designated Universal Cardholder Authentication Fields consistent with 3-D Secure protocols.

Patent EP1646976



Optimised to Fail: Card Readers for Online Banking

Drimer, Murdoch, and Anderson
Computer Laboratory, University of Cambridge



	CID	ATC	AC	IAD
Card output	80	A52D	AD452EF6BA769E4A	06770A03A48000
Bitmask	00	001F	000000000000FFFF	0000000000008000
Filter0D69E4A8...
Filter (binary)	0	1 101	0 110	1 001
Filter (hex)				1AD3C95
Decimal response				28130453

Field	Tag (hex)	Value (hex)
Terminal Country Code	9F1A	0000
Terminal Verification Results	95	8000000000
Transaction Currency Code	5F2A	0000
Transaction Date	9A	010101 for app. 0xA000000038002, 000000 for app. 0xA000000048002
Authorisation Response Code	8A	5A33
Other Amount	9F03	000000000000
Transaction Type	9C	00

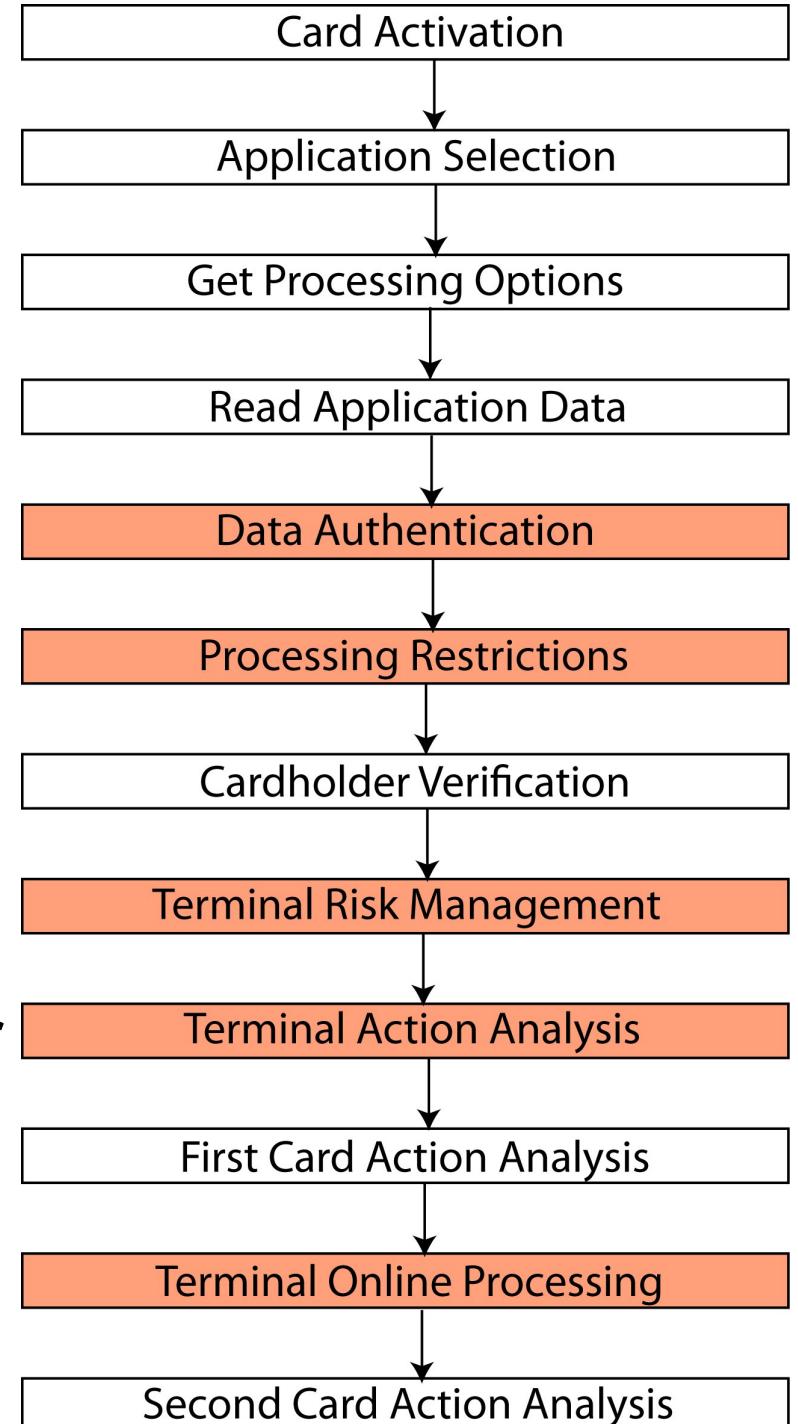
Dutch EMV-cards and Internet Banking

Thesis by Schouwenaar, Radboud University



EMV-CAP ~ Aborted EMV transaction

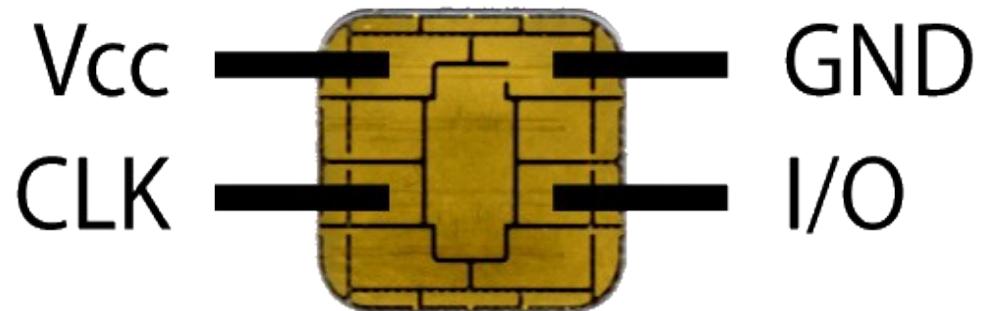
- EMV spec is public
- EMV-CAP not
- Different in UK, NL, BE,...
- M2 w. data is M2+TDS
- We managed to talk to our card and get responses
- But banks refuse our tokens :-)



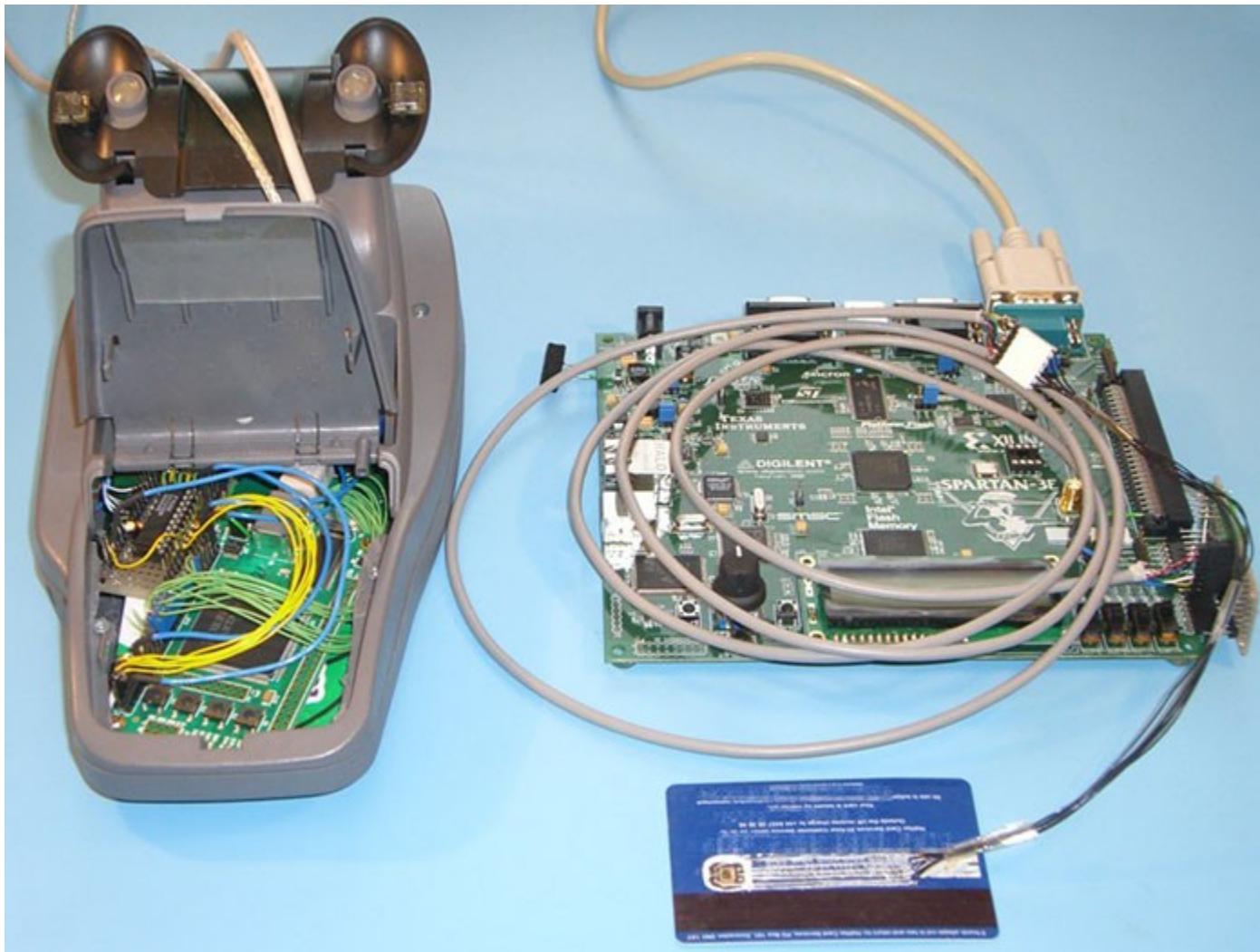


Interfaces

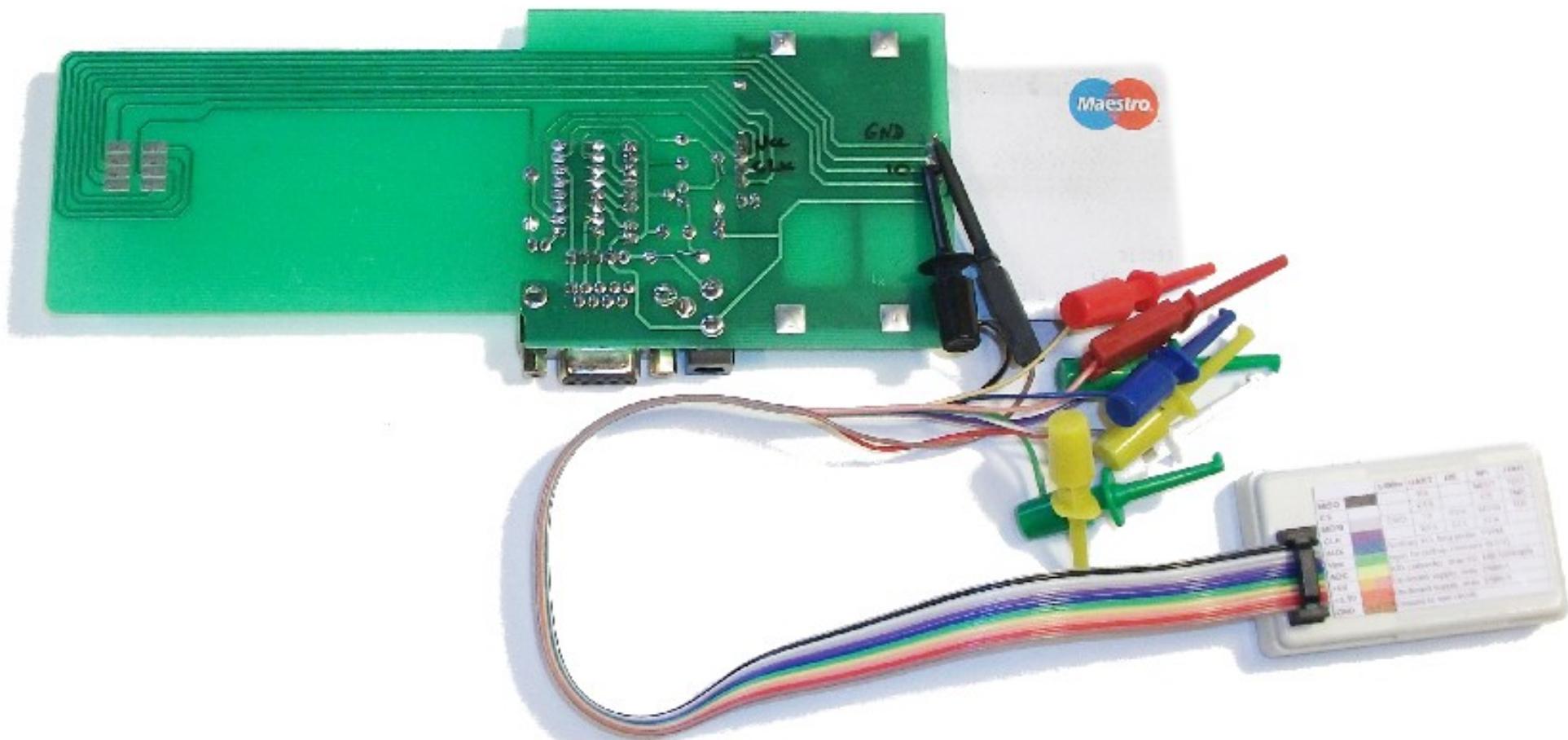
- UART, almost like RS232
- But only one I/O pin
- Arbitrary baudrate



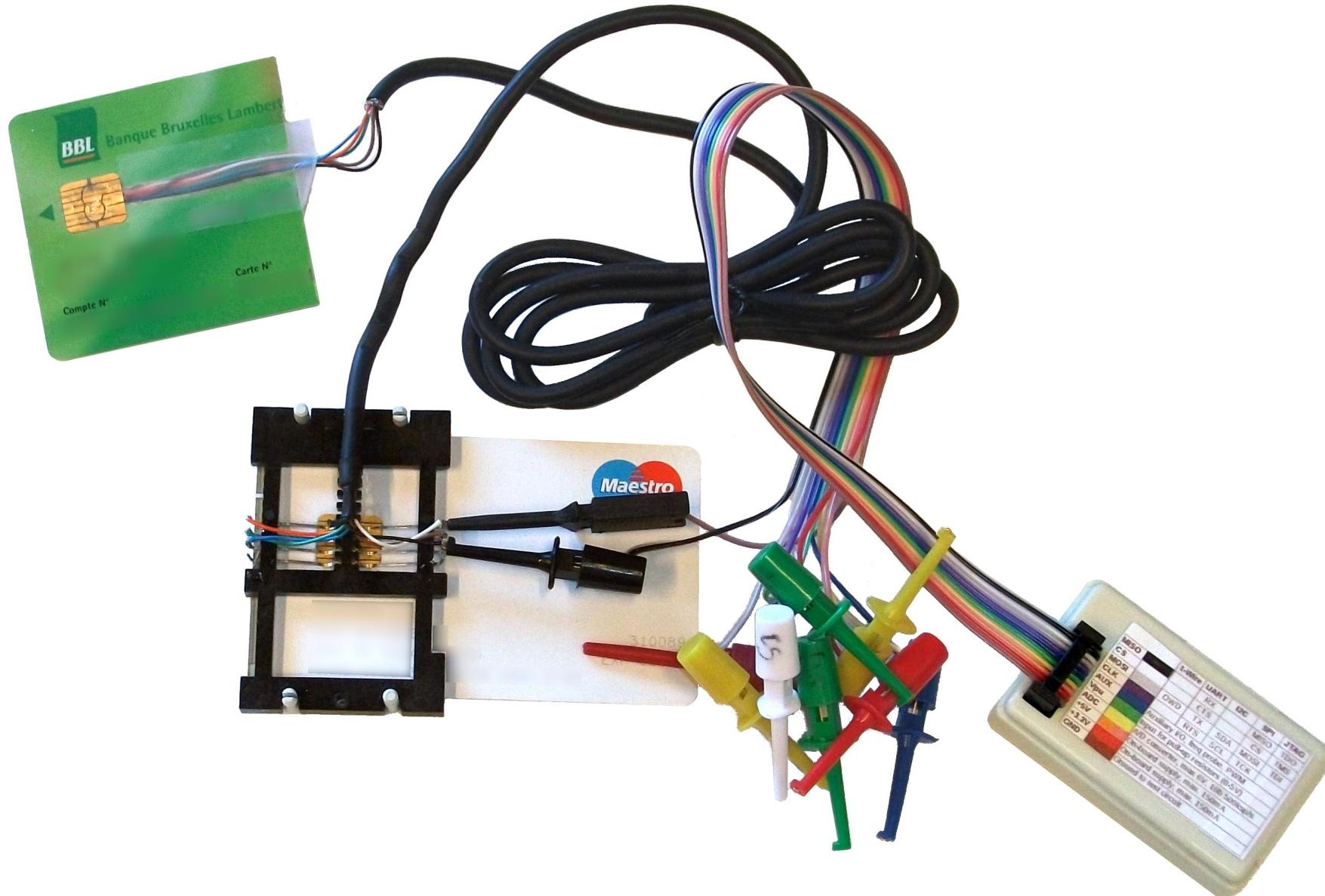
Using FPGA boards?



Go cheaper with Bus Pirate (& easier than programming Verilog)

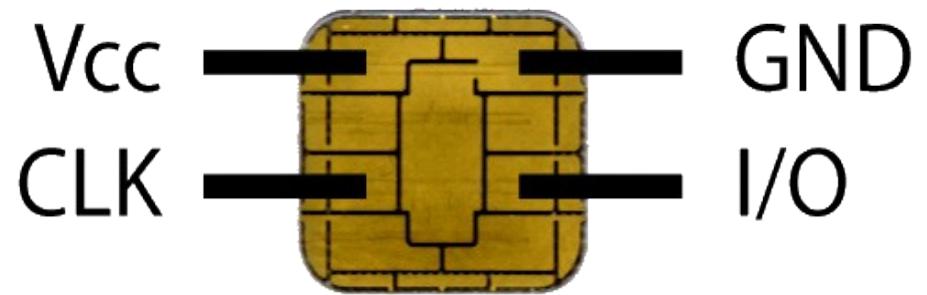


I said cheaper



Clockspeed? => Baudrate

Baudrate = clockspeed / 372



```
HiZ>i
Bus Pirate v3b
Firmware v5.10 (r559) Bootloader v4.3
DEVID:0x0447 REVID:0x3043 (24FJ64GA002 B5)
http://dangerousprototypes.com
HiZ>f
AUX Frequency: 1,495,552 Hz
```

=> 4020 bauds

UART>[

UART LIVE DISPLAY, } TO STOP

UART>

READ: 0x3B



3B:65:00:00:20:63:CB:6A:00:00:A4:04:00:07:A4:A0:00:00
:00:03:80:02:6A:82:00:A4:04:00:07:A4:A0:00:00:00:04:
0:02:6A:82:00:A4:04:00:08:A4:D0:56:00:06:66:11:10:10:
6A:82:...

READ: 0x65

UART>

READ: 0x00

\$ ATR_analysis 3B:65:00:00:20:63:CB:6A:00

UART>

READ: 0x00

ATR: 3B 65 00 00 20 63 CB 6A 00

UART>

+ TS = 3B --> Direct Convention

READ: 0x20

+ T0 = 65, Y(1): 0110, K: 5 (historical bytes)

UART>

READ: 0x63

TB(1) = 00 --> VPP is not electrically connected

UART>

TC(1) = 00 --> Extra guard time: 0

READ: 0xCB

+ Historical bytes: 20 63 CB 6A 00

UART>

Category indicator byte: 20 (proprietary format)

READ: 0x6A

00:A4:04:00:07:(A4):A0:00:00:00:03:80:02

UART>

6A:82

READ: 0x00

00:A4:04:00:07:(A4):A0:00:00:00:04:80:02

UART>

6A:82

00:A4:04:00:08:(A4):D0:56:00:06:66:11:10:10

6A:82

M1

- Challenge sent to the card in BCD
- Response:

CID	ATC	AC	IAD
80	005A	513C1201B7DB02A0	06015603A400000700030000010002

Issuer Proprietary Bitmap (IPB) :

00 00FF 00000000003FFFF

Filtered:

5A	302A0
----	-------

Binary:

01011010 110000001010100000

Decimal:

23790240 => correct!

We can now emulate M1!

BNP PARIBAS FORTIS | La banque et l'assurance d'un monde qui change

<Vous cherchez... ?> 

S'identifier comme client bpost banque

Numéro d'utilisateur : ? 02 762 20 00

Numéro de carte : ? 6703

Au sujet de BNP Paribas Fortis

Enregistrer les données de l'utilisateur sur cet ordinateur ?



1. Insérez votre **carte** et appuyez sur **M1**
'CHALLENGE ?' s'affiche.

2. Introduisez les 8 chiffres suivants : **9367 6112** > **OK**
'PIN ?' s'affiche.

3. Introduisez le **code de la carte** > **OK**
La signature électronique ('RESPONSE') s'affiche.

4. Introduisez ici la signature électronique. ? :

Numéro d'utilisateur ou numéro client : ? [Oublié votre numéro ?](#)

Module de sécurité : ? Lecteur de carte

Numéro de carte : ? 6703

Enregistrer les données de l'utilisateur sur cet ordinateur ?



1. Insérez votre **carte** et appuyez sur **M1**
'CHALLENGE ?' s'affiche.

2. Introduisez les 8 chiffres suivants : **1716 1953** > **OK**
'PIN ?' s'affiche.

3. Introduisez le **code de la carte** > **OK**
La signature électronique ('RESPONSE') s'affiche.

4. Introduisez ici la signature électronique. ? :



www.ing.be > Login to Home'Bank

Login to Home'Bank

 Beware of deceptive e-mails and phone calls

- > Never give out confidential personal details by telephone or via e-mail. This also applies to any combination ('RESPONSE') generated by your ING Card Reader.
- > Always log on to Home'Bank through www.ing.be

[More info](#)

1. Your details

ING ID 

Card ID 

Home'Bank Home'Bank Plus

Save my details

Password 

[New password](#) | [Forgot your password?](#)

2. Identification

1. Insert your ING bank card into the ING Card Reader and press 

2. Enter the pin of your ING bank card and press 

3. Enter the number appearing on the ING Card Reader screen, without spaces.

Confirmer

Home

Log-on box

Step-by-step instructions

Confirmer

Home

KBC-Online 

Card Number: 6703
Challenge: 5008 1077
Response:
 Save card number
Log-on
[How to login](#)
[Sign up for KBC-Online](#)
[Secure Internet banking](#)

Demo

1. In the log-on box

Type in the (17-digit) number on your KBC Bank Card.



You can also save the card number by selecting the Save card number check box. This will save you from having to type in this number again.



2. On your KBC Card Reader

- Insert your KBC Bank Card into the KBC Card Reader.
- Press .
- Copy the 8-digit 'CHALLENGE' you see in the log-on box and press .
- Enter the (4-digit) PIN for your KBC Bank Card and press .

3. In the log-on box

Step 6: Copy the (5 to 8-digit) 'RESPONSE' in the log-on box and press the log-on button.

M2 + TDS

- Challenge is 0000000000000000 ??
 - Card replies before you type the data ??
 - No visible correlation between card response cryptogram and actual OTP
 - Dutch thesis couldn't reverse M2+TDS
 - What happens in the device?
How data get mixed with card response to produce OTP?
- Need control over cryptogram

BROTHERS
PARKER

PROBLEMS TRADING GAME FROM PARKER BROTHERS®

MONOPOLY

BRAND

ELECTRONIC BANKING EDITION



AGES 8+
FAMILY

Monopoly Here & Now
problems of
featuring the

JavaCard Applet

We now control the cryptogram

PIN can be even used to control our fake card
and change cryptogram on-the-fly

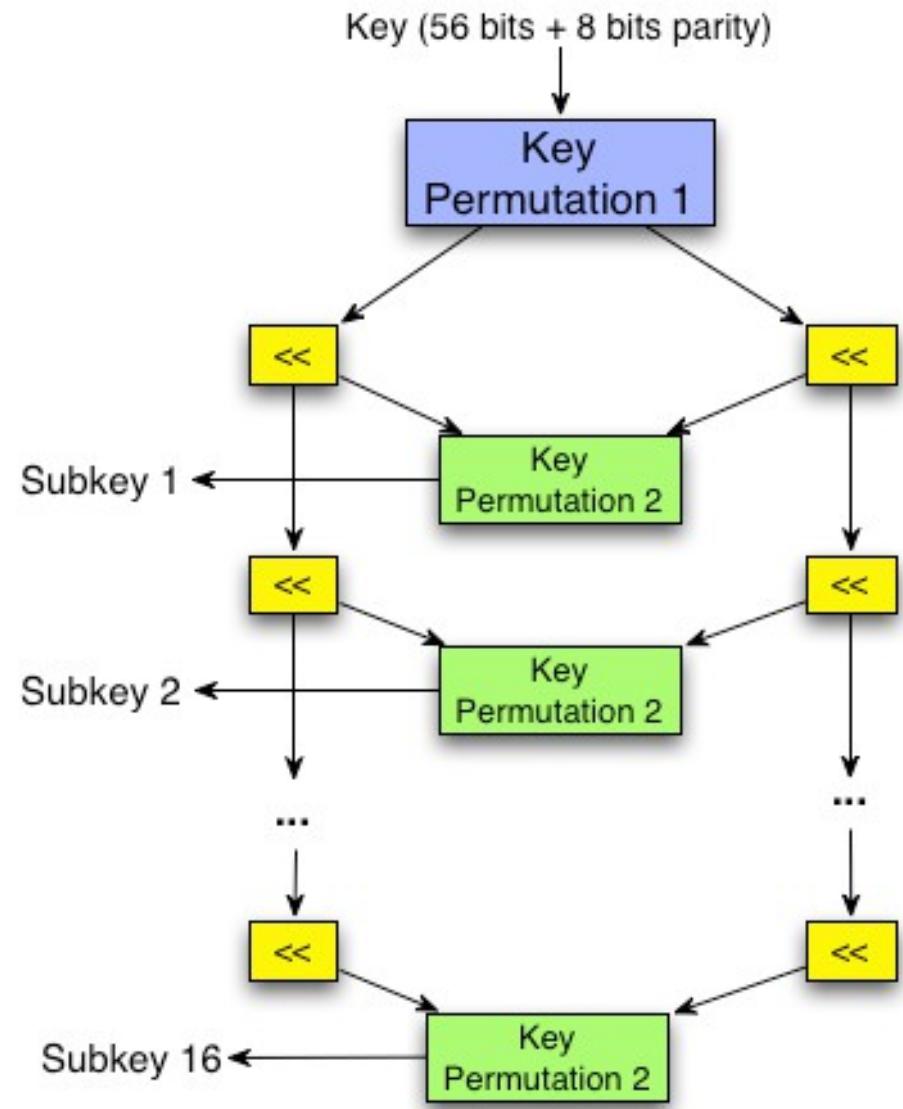
**Low bit of each byte
doesn't change OTP**



DES!

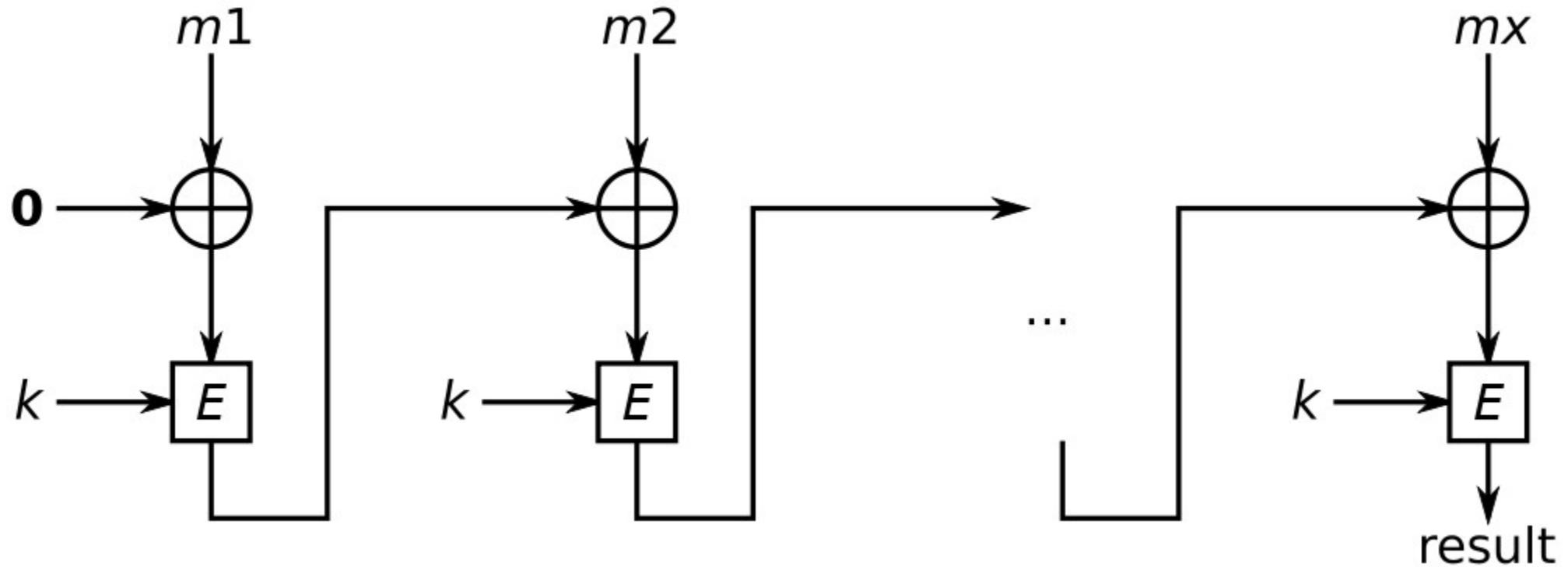
k=cryptogram AC

m=data in BCD
+ bit-padding



```
echo "1234800000000000" | xxd -r -p | \
openssl des-cbc -iv 0 -K $AC -nopad | xxd -p
```

DES CBC-MAC



If several data or ending on half byte
=> use 0xF as separator
E.g. 1234 & 5678:

1234F5678F800000

We can now emulate M2+TDS!

Virement Européen

Date d'exécution:

Montant:

Compte donneur d'ordre:

Donneur d'ordre:

Compte bénéficiaire:

Nom du bénéficiaire:

BIC de la banque bénéficiaire:

Communication:

Bénéficiaires sauvegardés

Alias:

Nom:

Numéro de compte (IBAN): BE84 230 03242 1300



1. Insérez votre carte et appuyez sur **M2**
'PIN ?' s'affiche.
2. Introduisez le code de la carte > **OK**
'DATA OR OK ?' s'affiche.
3. Introduisez les chiffres suivants correspondant à votre transaction :
Montant (décimales incluses) **25 00** > **OK** > Bénéficiaire **84 2300 3242** > **OK** > **OK**
La signature électronique ('RESPONSE') s'affiche.
4. Introduisez ici la signature électronique. **?** :



Uranium Ore

By

 (291 customer reviews) |  (349)

Price: \$39.95

In stock.

Processing takes an additional 4 to 5 days for orders from this seller.
Ships from and sold by [Images SI Inc.](#).

Ordering for Christmas? Based on the shipping schedule of Images SI Inc., details.

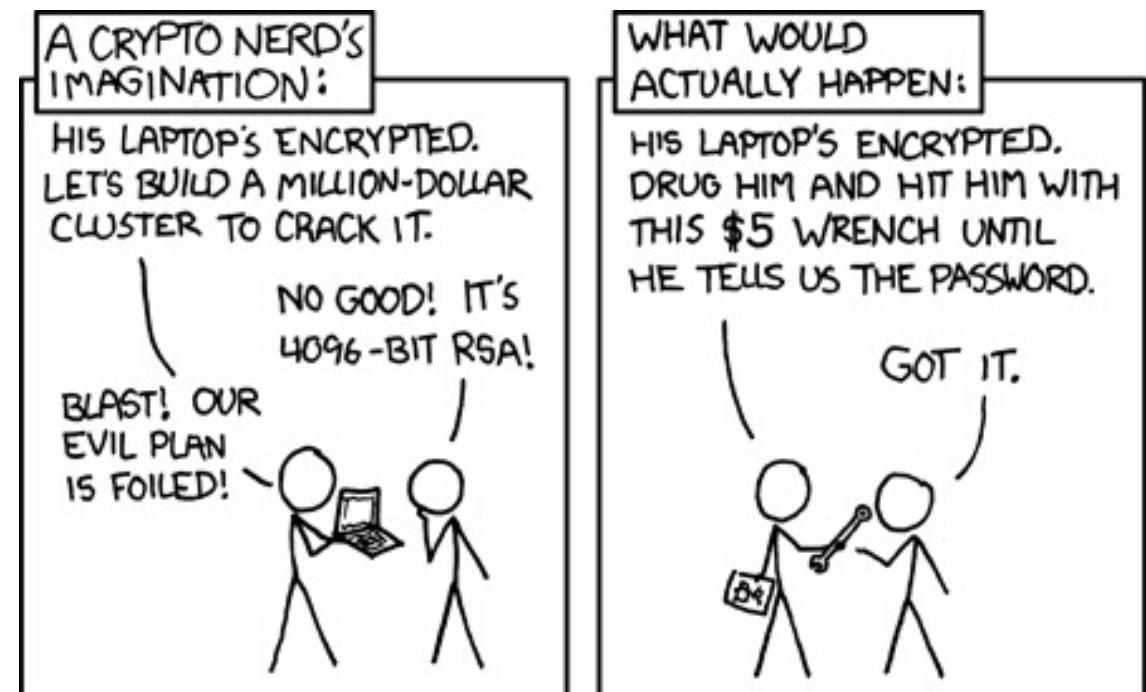


More Lab & Safety Supplies

Find a [radiation detector](#), [geiger counter](#) plus other [safety supplies](#) in our [Industrial Supplies store](#).

State of the union

- EMV-CAP safer than EMV
- EMV-CAP M2+TDS better than foreseen
- But EMV-CAP devices could be used to validate PIN



Still a funny fact

- Collect cryptograms from null challenges
- Get card swollen by your bank ATM
- Use cryptograms to buy on Internet
- Contest, pretend it couldn't be you
- Pretend you weren't at Hack.lu 2013...

Would have been better with timer instead of counter

MAKE



```
$ EMV-CAP -h
```

```
usage: EMV-CAP [-h] [-l] [-L] [--tlv PARSETLV]
                [-r {<index>, <reader_substring>}] [-d] [-v] [-m {1,2}]
                [--warmreset {auto,yes,no}]
                [N [N ...]]
```

EMV-CAP calculator

optional arguments:

-h, --help show this help message and exit

Standalone options:

-l, --listreaders print list of available readers and exit

-L, --listapps print list of available applications on the card and exit

--tlv PARSETLV parse a hex string into TLV elements

Global options:

-r {<index>, <reader_substring>}, --reader {<index>, <reader_substring>}
 select one specific reader with reader index, name
 string or sub-string otherwise first reader found will be used.

-d, --debug print exchanged APDU for debugging

-v, --verbose print APDU parsing

Modes and data:

-m {1,2}, --mode {1,2}
 M1/M2 mode selection (mandatory, unless -l or -L is used)

N
 number(s) as M1/M2 data: max one 8-digit number for M1
 and max 10 10-digit numbers for M2

--warmreset {auto,yes,no}
 Warm reset: yes / no / auto (default) If 'auto' it
 will perform a warm reset if the ATR starts with 3F
 (indirect convention)

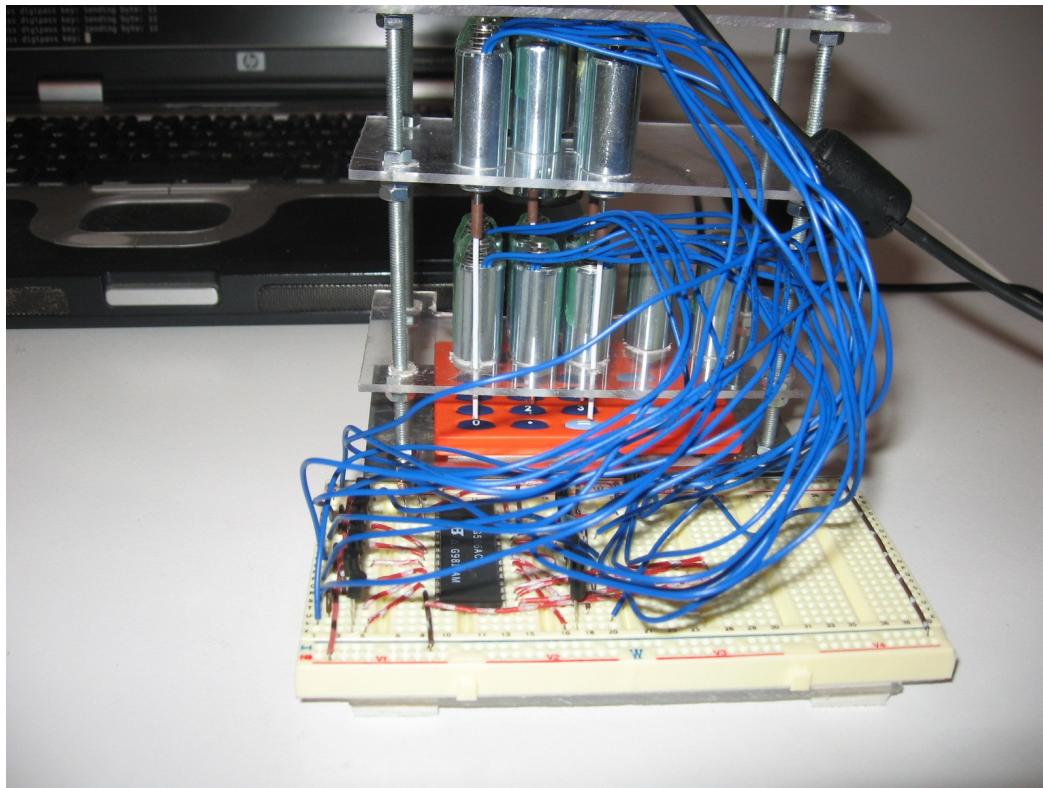
Dangerous confort!



Those devices were made to isolate
your card and PIN entry from
malwares, remember?

Could still be useful to some...

LimID



Adrian

Resources

- <http://sites.uclouvain.be/EMV-CAP/>
- <http://www.unixgarden.com/index.php/misc/banques-en-ligne-a-la-decouverte-demv-cap>

Credits

- Jean-Pierre Szikora
- Philippe Teuwen
- Michaël “keccak” Peeters

Are we done?

DIGIPASS 810 - VASCO

shop.vasco.com/digipass_810_detail.aspx

 DIGIPASS 810 eID
12.49 €
incl. VAT / piece
incl. Recupel
in Stock

More info at www.mydigipass.com
Leaflet [download here](#).

DIGIPASS 810 eID enables convenient and secure log in to MYDIGIPASS.COM with your Belgian eID card.

- Unconnected and portable eID reader.
- No software installation needed.

1 Piece(s)

Add to Basket

FR NL SHOPPING CART (0)

PRODUCTS SUPPORT VASCO

DIGIPASS 810 eID
enables convenient
and secure log in to
MYDIGIPASS.COM
with your Belgian
eID card





Authentifiez votre DIGIPASS

Numéro de série du DIGIPASS

Code d'enregistrement

S'authentifier

Generez votre code d'enregistrement

- 1 Insérez votre carte d'identité dans le lecteur de carte et sélectionnez Enregistrer
- 2 Entrez le code PIN de votre ID électronique, puis appuyez sur OK

Vos informations personnelles

Prénom

Nom de famille

Pays

Belgique

Adresse e-mail

nom@domaine.com

Date de naissance

Jour Mois Année

You devez avoir au moins 14 ans pour vous inscrire

Votre clé principale personnelle

Cette clé est utilisée pour crypter vos données personnelles et est requise pour récupérer votre compte. Créez une clé principale facile à retenir, par ex. une ligne de votre chanson ou poème préféré(e).

Votre clé principale personnelle

Confirmez votre clé principale personnelle

En vous inscrivant, vous acceptez les [Conditions d'utilisation](#) et notre [Déclaration de confidentialité](#).

Inscription

Enregistrez votre DIGIPASS pour créer votre compte.

Wait a moment

- eID = RSA signature, not symm. encryption
- 1024-bit signature
- Pk = certificate checking
- eID certificate never asked by Mydigipass.com
- Still all goes via short digital OTPs

Using same weapons

- Certificate never read
 - eID always signs ZEROES! → output constant
 - Yes, a javacard clone is stupidly easy to do
-
- Digipass contains timer
 - Digipass contains secret



+



=



+



Today (well, last week)

From Alex Ongena <Alex.Ongena@vasco.com>★

Reply

Forward

Archive

Junk

Delete

ABP

Subject MYDIGIPASS.COM - eID based reader - product discontinued

03:33 PM

To phil@teuwen.org★



Other Actions▼

Dear MYDIGIPASS.COM User,

You receive this e-mail as you have been registered in <https://www.mydigipass.com> with a VASCO 810 eID reader product.

SN 3200011500

SN 3200011470

This product was tagged "VASCO internal release only" version and distributed to a limited number of users for evaluation purposes.

Earlier this year, VASCO decided to not release the product to the market.

Access to your MYDIGIPASS.COM account, using this product, is no longer supported. You can either login via the Backup Solution (follow 'I forgot my DIGIPASS') or other supported DIGIPASS.

A free Mobile DIGIPASS can be obtained via Apple iTunes or Google Play added to your existing account.

VASCO internal release only?!?



Next step: digipass+eID v2

- Digipass 870
- Reviewed by FedICT and COSIC
- Can be USB-connected
- Vasco, please send me one now that I lost 25€



Guessing the protocol...

- eID certificate is known by server
 - Server can check certificate chain etc
- Digipass
 - read certificate
 - send random data to be signed
 - verify signature
 - hash certificate & mix with internal OTP → OTP2
- Server
 - get OTP2
 - can do same hash cert mix + OTP and check

Thank you