UNIVERSITY OF CAMBRIDGE

Security Protocols and Evidence: Where Many Payment Systems Fail

Steven J. Murdoch, Ross Anderson

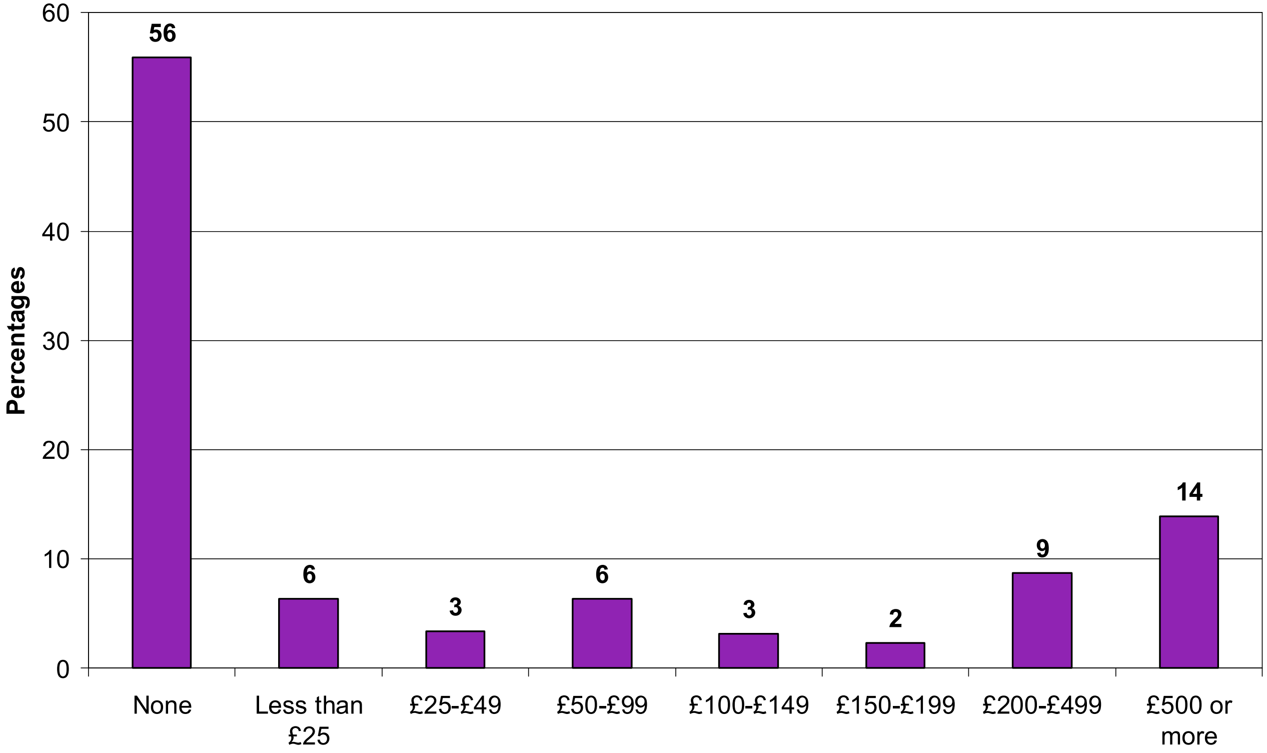
Computer Laboratory

Fraud prevention techniques and incentives

- Chip and PIN was never intended to eliminate fraud, but it was designed to keep levels under control
- Banks continually have to make risk decisions as to how much to spend to reduce fraud
  - Money spent building and maintaining the system
  - Inconvenience to customers (false positives, new procedures)
  - Reputational damage from admitting that better security is needed
- Banks make (or lose) their money by balancing risks
- While banks pay the for their decisions, we can hope for good results

Do banks pay for fraud losses?

- The 2008/2009 British Crime Survey found that 44% of fraud victims didn't get all their money back



What rules apply to dispute resolution in the EU?

- Draft Payment Services Directive (2005)

> “ the use of a payment verification instrument recorded by the payment service provider shall not, of itself, be sufficient to establish either that the payment was authorised by the payment service user or that the payment service user acted fraudulently or with gross negligence

- Payment Service Directive as passed (2007)

> “ the use of a payment instrument recorded by the payment service provider shall in itself not **necessarily** be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence

Why was there a change?

- Submission from Barclays to EU (2002)

> “Our contract with the customer states that **our records will be used as conclusive evidence** except in the case of obvious errors. This means that we have a duty to prove that a payment transaction has been accurately executed but that our records can be regarded as good evidence. **We would not wish to see any weakening in the evidential integrity of our records**.”

- Bankers’ Books Evidence Act (1879)

> “Subject to the provisions of this Act, a copy of **any entry in a banker’s book shall in all legal proceedings be received as prima facie evidence of such entry**, and of the matters, transactions, and accounts therein recorded.”

Dispute resolution

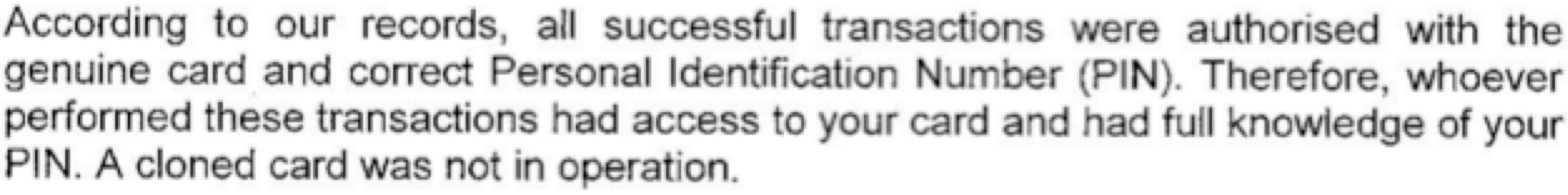
- Most countries have a standard set of procedures for dealing with disputes
  - Internal Dispute Resolution
  - Alternative Dispute Resolution (ADR)
  - Court system
- There are variations between systems
  - Only some banks combine fraud investigation and dispute resolution
  - ADR may not exist, be optional or be mandatory
  - There may be multiple levels of the court system and who pays cost

Why might bank records be inaccurate?

- Protocol flaw
  - e.g. No-PIN attack
- Technical failure
  - e.g. Fallback transaction recorded as Chip and PIN
- Insider attack
  - e.g. issue of duplicate cards
- Incomplete records
  - e.g. information needed to verify decision has been destroyed

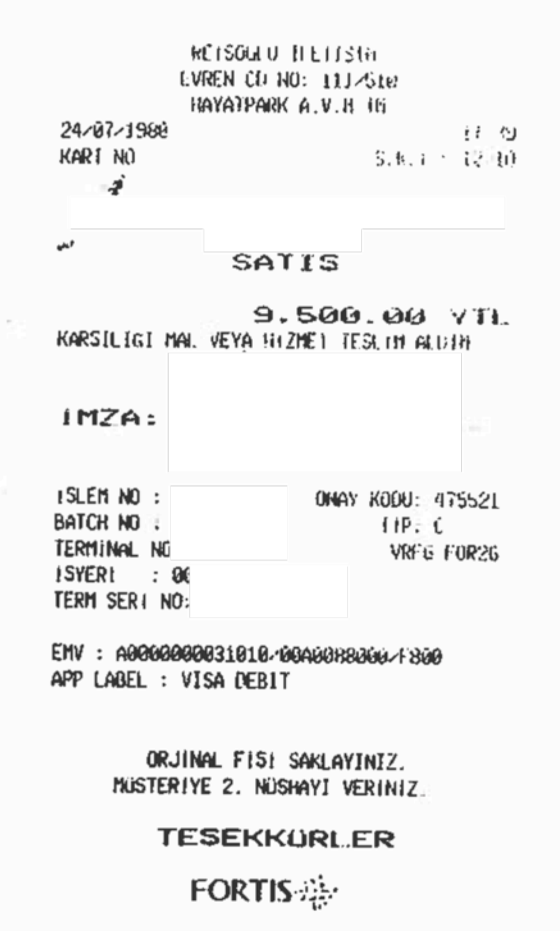
Turkey case evidence

“



According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.

Turkey case verification



KEISOGLU ILETISIM
EVREN CD NO: 11J/Ste
HAYATPARK A.V.M IG

24/07/1988 [illegible]
KART NO S.K.T : 12 10

[redacted]

SATIS

9.500.00 YTL
KARSILIGI MAL VEYA HIZMET TESLIM ALDIM

IMZA: [redacted]

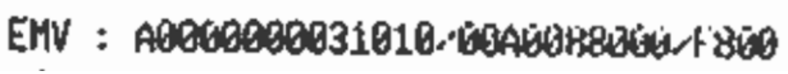
ISLEM NO : [redacted] ONAY KODU: 475521
BATCH NO : TIP: C
TERMINAL NO VRFG FOR2G
ISYERI : 00[redacted]
TERM SERI NO:

EMV : A0000000031010/00A0088000/F800
APP LABEL : VISA DEBIT

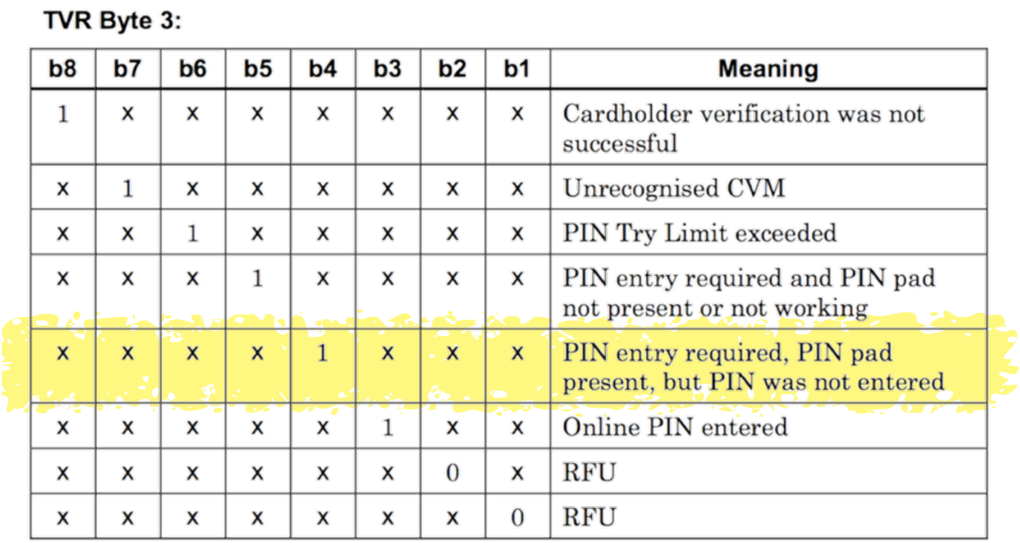
ORJINAL FISI SAKLAYINIZ.
MUSTERIYE 2. NUSHAYI VERINIZ.

TESEKKURLER

FORTIS



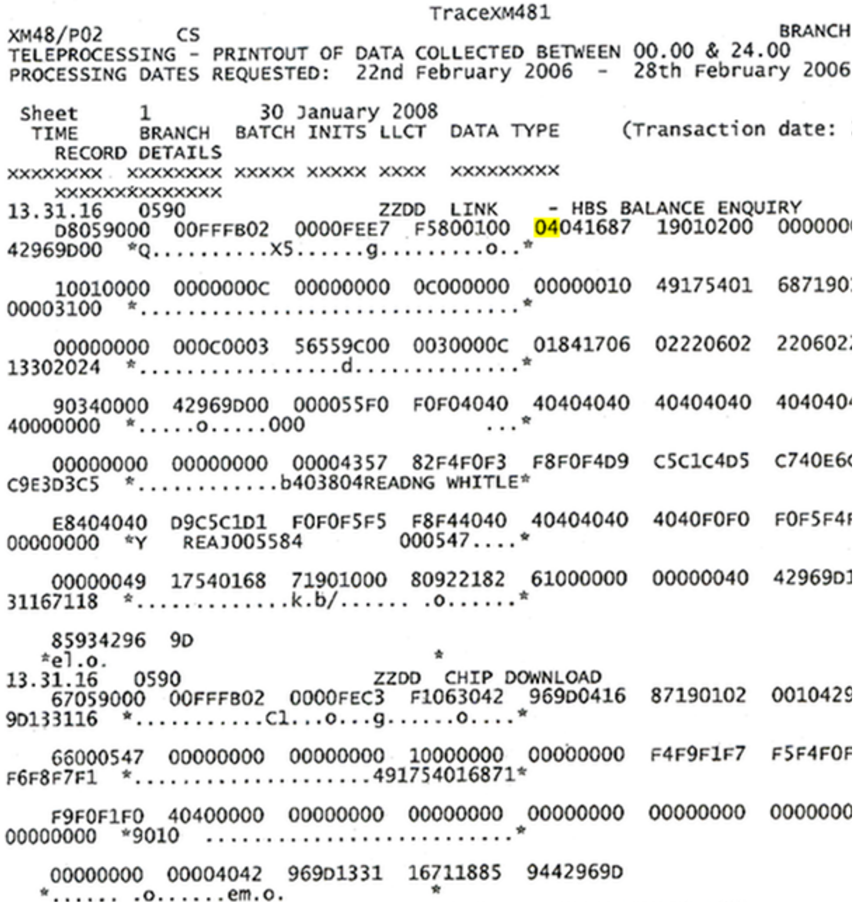
EMV : A0000000031010/00A0088000/F800



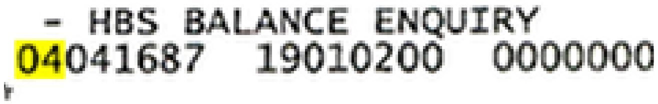
TVR Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cardholder verification was not successful
x	1	x	x	x	x	x	x	Unrecognised CVM
x	x	1	x	x	x	x	x	PIN Try Limit exceeded
x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or not working
x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
x	x	x	x	x	1	x	x	Online PIN entered
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Job case evidence

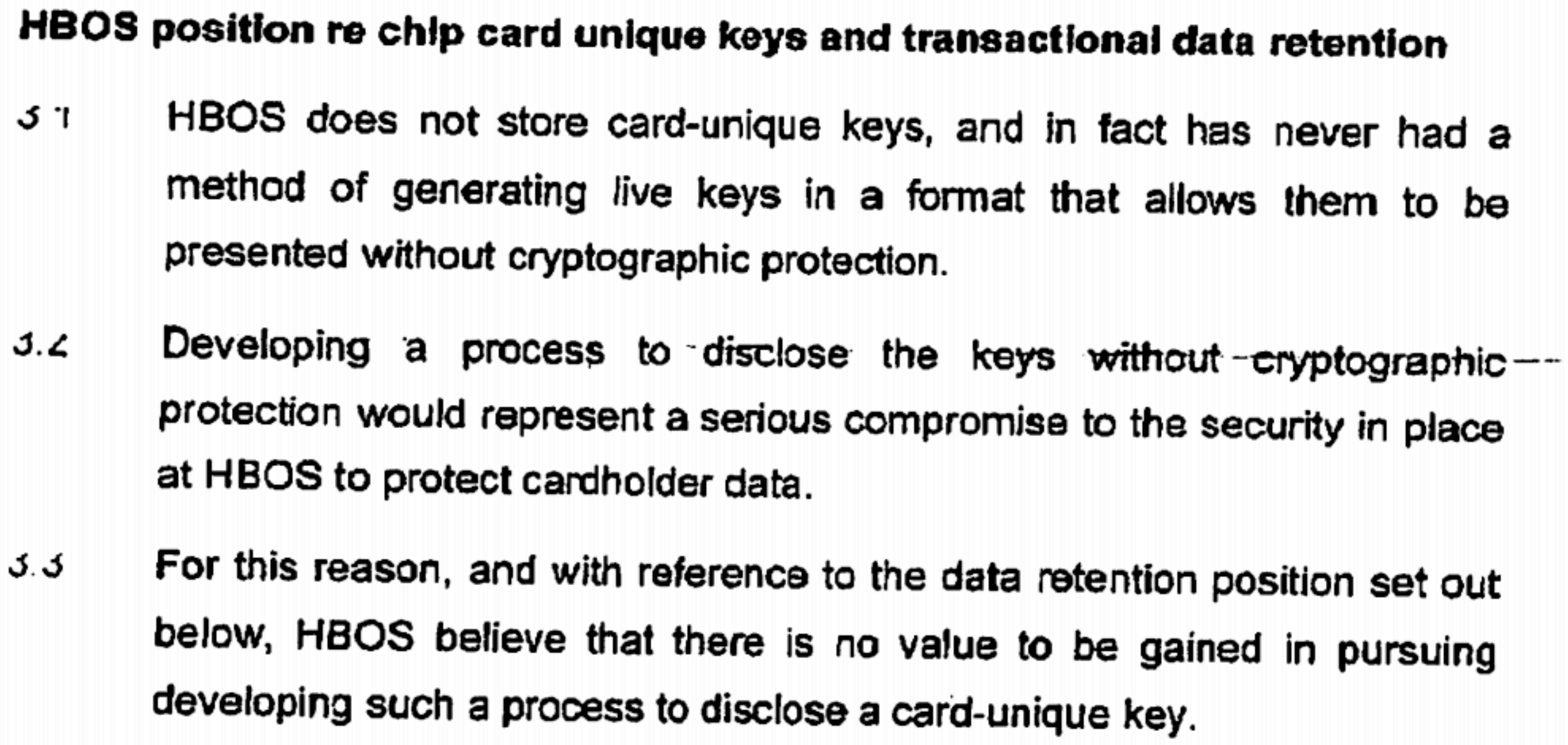


```
                                     TracexM481
XM48/P02      CS                                                 BRANCH
TELEPROCESSING - PRINTOUT OF DATA COLLECTED BETWEEN 00.00 & 24.00
PROCESSING DATES REQUESTED:  22nd February 2006  -  28th February 2006

 Sheet      1         30 January 2008
  TIME     BRANCH  BATCH INITS LLCT  DATA TYPE      (Transaction date:
    RECORD DETAILS
xxxxxxxx  xxxxxxxx xxxxx xxxxx xxxx  xxxxxxxxx
    xxxxxxxxxxxxxx
13.31.16   0590                ZZDD  LINK     - HBS BALANCE ENQUIRY
    D8059000  00FFFB02  0000FEE7  F5800100  04041687  19010200  000000
42969D00  *Q..........X5......g.........o..*

    10010000  0000000C  00000000  0C000000  00000010  49175401  687190
00003100  *................................*

    00000000  000C0003  56559C00  0030000C  01841706  02220602  220602
13302024  *.................d..............*

    90340000  42969D00  000055F0  F0F04040  40404040  40404040  404040
40000000  *.....o.....000                ...*

    00000000  00000000  00004357  82F4F0F3  F8F0F4D9  C5C1C4D5  C740E6
C9E3D3C5  *............b403804READNG WHITLE*

    E8404040  D9C5C1D1  F0F0F5F5  F8F44040  40404040  4040F0F0  F0F5F4
00000000  *Y   REAJ005584          000547....*

    00000049  17540168  71901000  80922182  61000000  00000040  42969D1
31167118  *.............k.b/...... .o......*

    85934296  9D
   *el.o.                          *
13.31.16   0590                ZZDD  CHIP DOWNLOAD
    67059000  00FFFB02  0000FEC3  F1063042  969D0416  87190102  0010429
9D133116  *............Cl...o...g......o....*

    66000547  00000000  00000000  10000000  00000000  F4F9F1F7  F5F4F0F
F6F8F7F1  *....................491754016871*

    F9F0F1F0  40400000  00000000  00000000  00000000  00000000  0000000
00000000  *9010  .........................*

    00000000  00004042  969D1331  16711885  9442969D
   *...... .o......em.o.            *
```



```
 - HBS BALANCE ENQUIRY
04041687  19010200  0000000
```

Job case verification?



HBOS position re chip card unique keys and transactional data retention

3.1 HBOS does not store card-unique keys, and in fact has never had a method of generating live keys in a format that allows them to be presented without cryptographic protection.

3.2 Developing a process to disclose the keys without cryptographic protection would represent a serious compromise to the security in place at HBOS to protect cardholder data.

3.3 For this reason, and with reference to the data retention position set out below, HBOS believe that there is no value to be gained in pursuing developing such a process to disclose a card-unique key.

Designing for evidence

- EMV fails to produce evidence which is in practice
  - Reliable
  - Verifiable
  - Repeatable
- When EMV disputes occur the outcome can be unfair
  - Customers may lose because they get the blame for fraud
  - Banks may lose because they refund fraudulent disputes
  - Criminals may win because fraud is written off as customer negligence and not reported to the police

Design Principles

Principle 1: Retention and disclosure. Protocols designed for evidence should allow all protocol data and the keys needed to authenticate them to be publicly disclosed, together with full documentation and a chain of custody.

- Don’t delete logs!
- Keep logs on card
  - Creates a privacy risk
- Allow verification of cryptograms
  - New HSM instructions risk introducing bugs

Design Principles

Principle 2: Test and debug evidential functionality. When a protocol is designed for use in evidence, the designers should also specify, test and debug the procedures to be followed by police officers, defence lawyers and expert witnesses.

- Currently no accepted procedures for dealing with EMV evidence
  - Increased cost to the court system as experts need to agree
  - Cards have lots of issuer-specific behaviour which could assist
- Collecting evidence from EMV cards is not repeatable
  - Need to first start a transaction

Design Principles

Principle 3: Open description of TCB. Systems designed to produce evidence must have an open specification, including a concept of operations, a threat model, a security policy, a reference implementation and protection profiles for the evaluation of other implementations.

- Currently the TCB for EMV dispute resolution is huge
  - Card firmware
  - Bank transaction processing system, HSM and logging
  - Everything connected: Internet banking, marketing, call center

Design Principles

Principle 4: Failure-evidentness. Transaction systems designed to produce evidence must be failure-evident. Thus they must not be designed so that any defeat of the system entails the defeat of the evidence mechanism.

- Repeating existing checks adds little
  - If dispute occurs, transaction happened, so checks should have been done already
- We need to have a security mechanism which is checked only if there is a dispute

Design Principles

Principle 5: Governance of forensic procedures. The forensic procedures for investigating disputed payments must be repeatable and be reviewed regularly by independent experts appointed by the regulator. They must have access to all security breach notifications and vulnerability disclosures.

- Procedures may need to change to adapt to known threats
- It must be possible to repeat checks to allow for opposing expert witnesses and appeals
- Ensuring that dispute resolution works is the role of the regulator

Pulling it all together

- Audit log on card with separate keys from transaction ones
  - Logs also stored at bank in case card is lost or destroyed
  - Small TCB, can be freely disclosed (Principles 1 and 3)
- Develop, test and maintain procedures for checking available logs
  - Requires bank so store logs (Principles 2 and 5)
- Checks can only be performed when card in forensics mode
  - Repeatable, privacy preserving (Principles 4 and 5)
- Can be incrementally deployed without new cards and only requires changes by a single issuer

Other systems

	Retention & Disclosure	Test and debug procedures	Open TCB	Failure-evidentness	Governance
Phone banking	✗	✗	✗	✗	✗
Sofortüberweisung	✓	✗	✗	✗	—
Bitcoin	✓	✗	✓	✗	✗

Conclusions

- If we don’t want protocols an implementations to be terrible, the party which designs and maintains them must pay the cost for their failure
- Dispute resolution is necessary to achieve this goal and needs to be thought of from the beginning of protocol design:

1. All protocol data and the keys to authenticate them can be disclosed
2. Specify, test and debug the forensic procedures to be followed
3. Systems designed to produce evidence must have an open TCB
4. Any defeat of the system must not defeat the evidence mechanism
5. Forensic procedures must be repeatable and be reviewed regularly