Payment System

Security Engineering

Dr Steven J Murdoch
University College London

Security Engineering

- “Building systems to remain dependable in the face of **malice**, error or mischance” (Security Engineering, Anderson)
- Shares similarities with systems engineering
  - e.g. attacks exploit bugs, and systems engineering seeks to avoid bugs
- However some systems engineering approaches and tools don’t apply
  - e.g. it is an incorrect to assume probabilities of failure are independent when an attacker may trigger them

Security properties

- **C**onfidentiality
  - Only authorised people would have the ability to **view** confidential information
- **I**ntegrity
  - Only authorised people would have the ability to **change** confidential information, and the **identity** of who created/changed something can be established
- **A**vailability
  - Legitimate actions are not prevented

Threat modelling

- A systematic approach to answering the following questions:
  - What are the capabilities of the potential **adversaries**?
  - What **assets** needs to be protected
  - How can this level of protection can be achieved

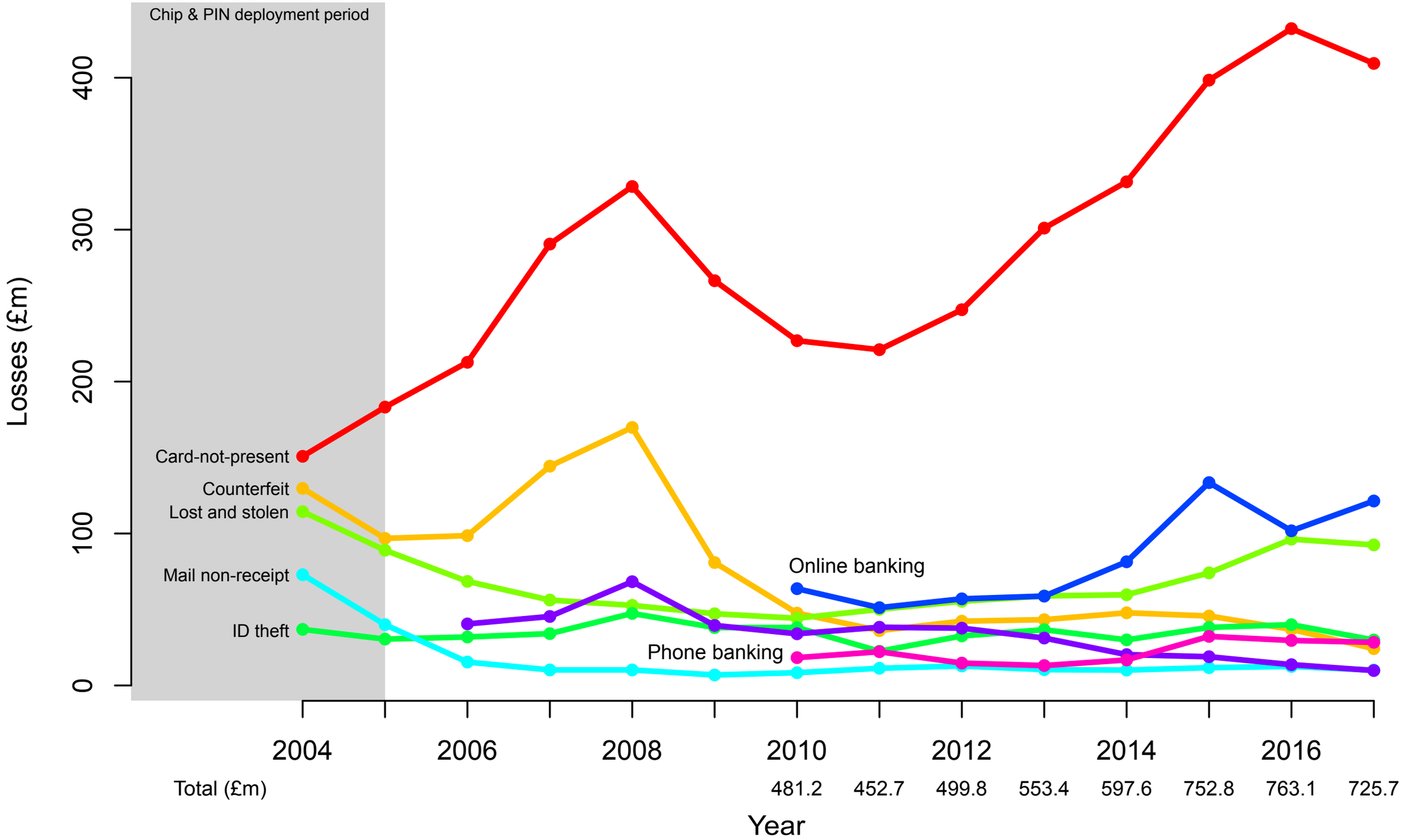
STRIDE model (Microsoft)

- **S**poofing identity
- **T**ampering with data.
- **R**epudiation
- **D**enial of service
- **E**levation of privilege

Example security mechanisms

- **Access control** (e.g. ACLs, file permissions)
  - A system has a policy which permits some things but prevents some other things. Someone has to set up the system and (initial) policy
- **Cryptography** (encryption, authentication, and more)
  - Moves control over data from where it is to where it needs to be
- **Tamper resistance**
  - Access control and cryptographic protections continue to work even if adversary has physical access

UK fraud went down last year



But that's only part of the story

- **Lost and Stolen fraud volume went up by 51%**
  - From 231,000 cases to 350,000
    - Likely due to lack of full set of security checks in contactless transactions
- **Online banking fraud went up by 19%**
  - From £101.8 million to £121.4 million
- These statistics cover transactions where the bank is liable to pay the cost of fraud

Push payment scams were hidden from fraud statistics

- **Banks started counting in 2017 after pressure from the regulator**
  - This was the result of a campaign by Which?
- Losses of £236 million for 44,000 cases
  - **Over £5,000 per case**
  - Liability falls on customer, under current rules

Chip and PIN transactions have three main stages

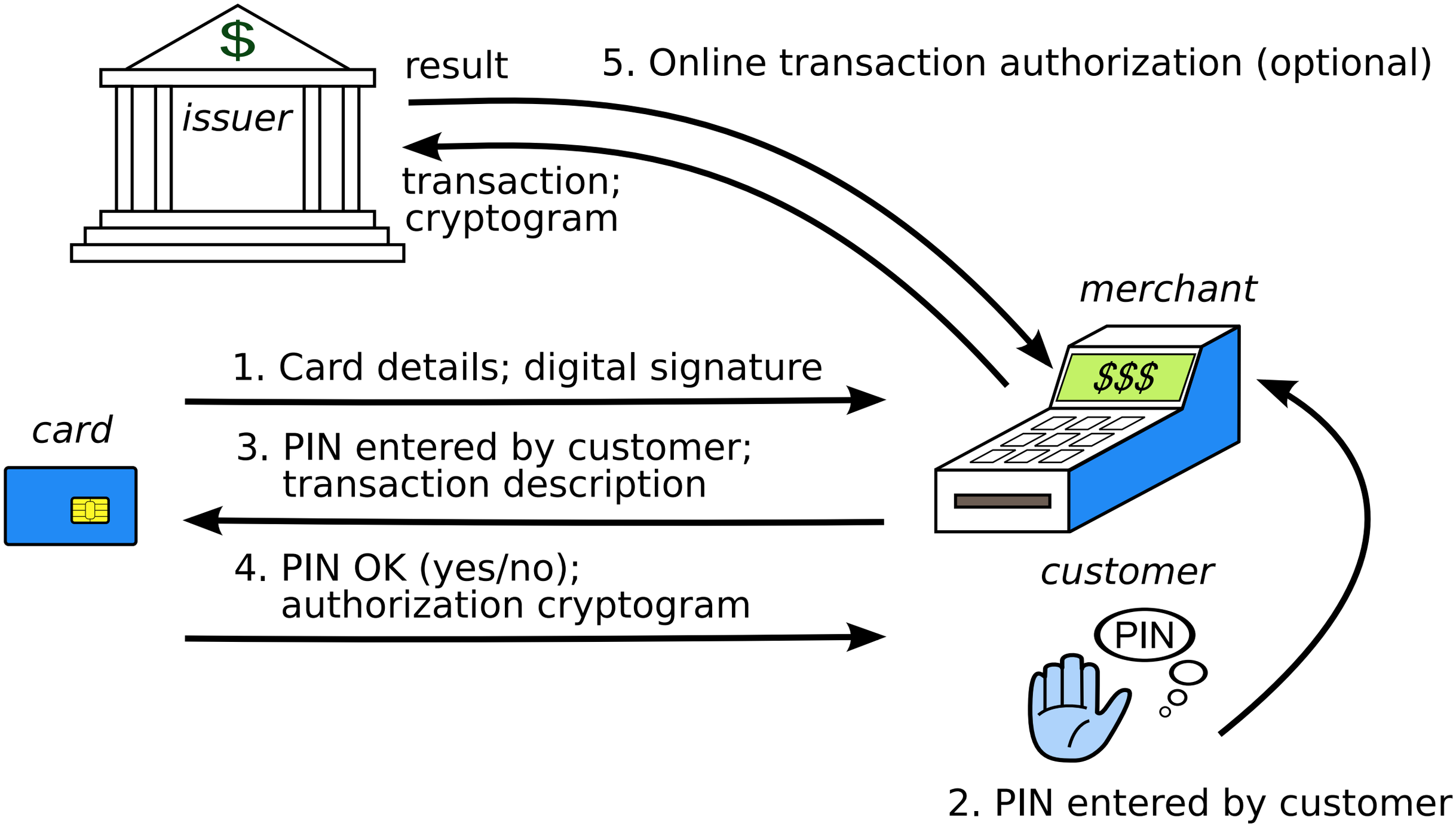
- **Card authentication**
  card proves it is real through providing a digital signature that the terminal can verify

- **Cardholder verification**
  card and terminal check that legitimate cardholder is present (normally by card verifying the PIN)

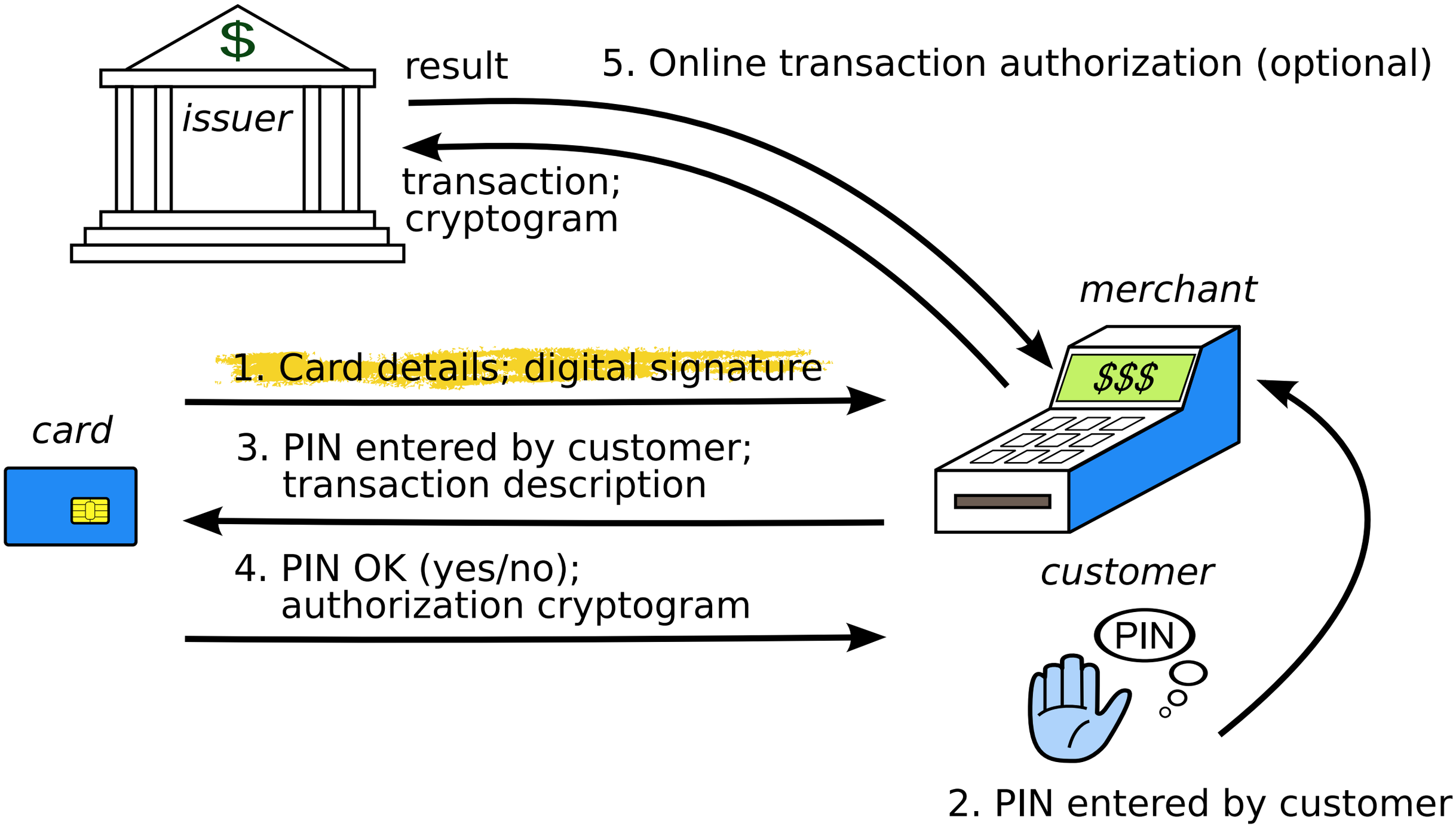
- **Transaction authorisation**
  terminal checks with bank that previous steps have been followed and the transaction should proceed

EMV protocol

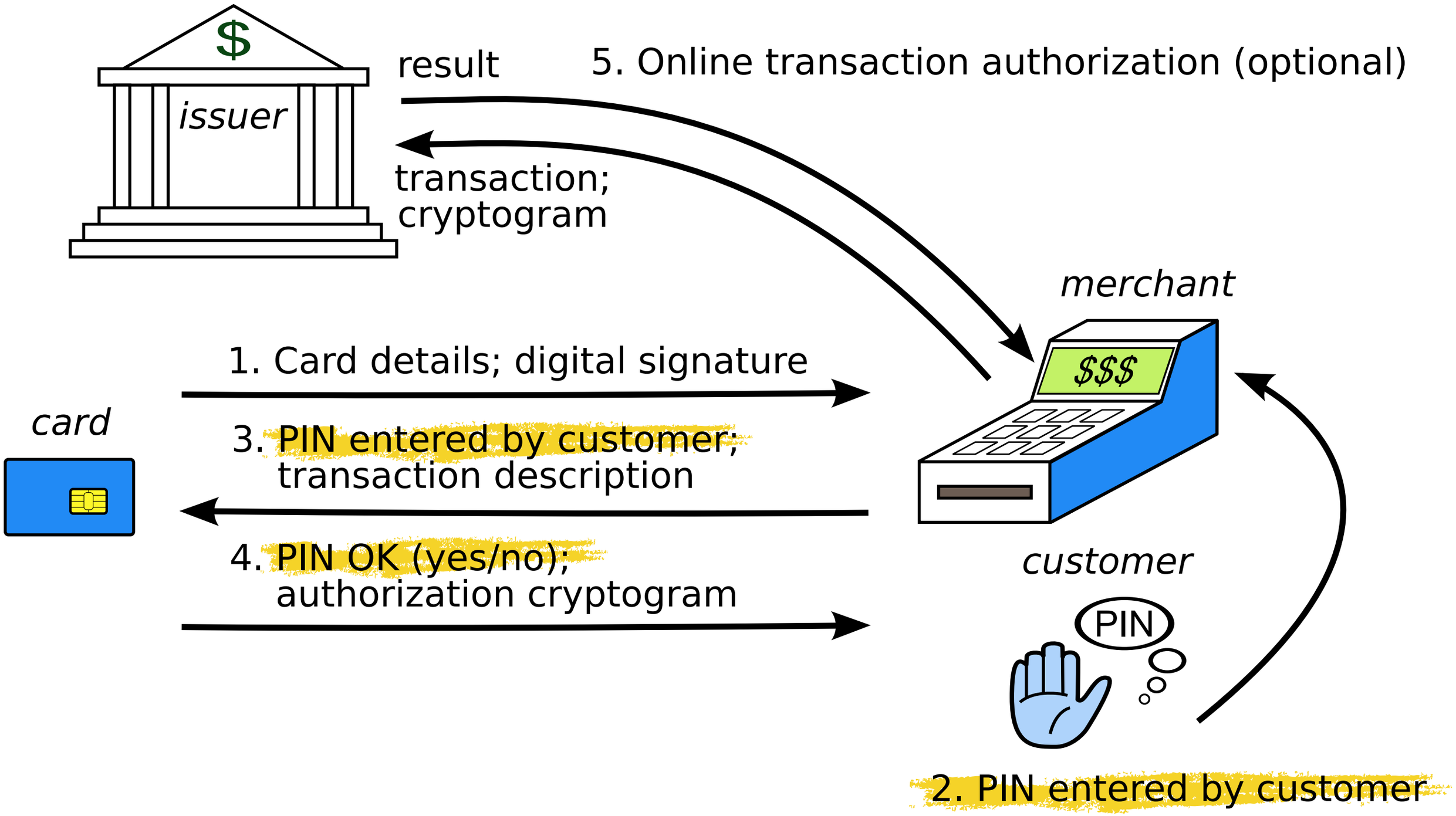
- **Card authentication**
- **Cardholder verification**
- **Transaction authorisation**



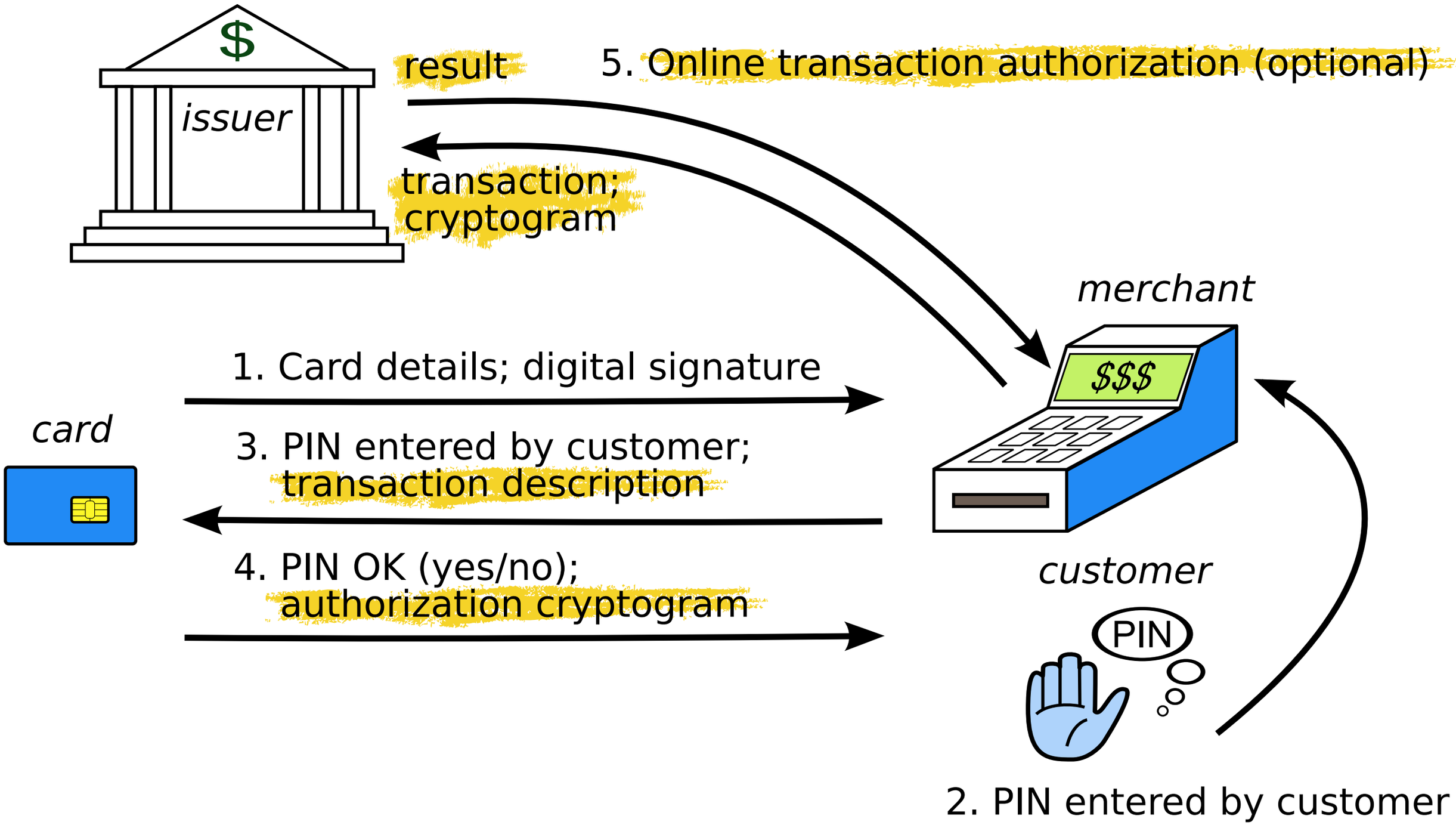
Card authentication



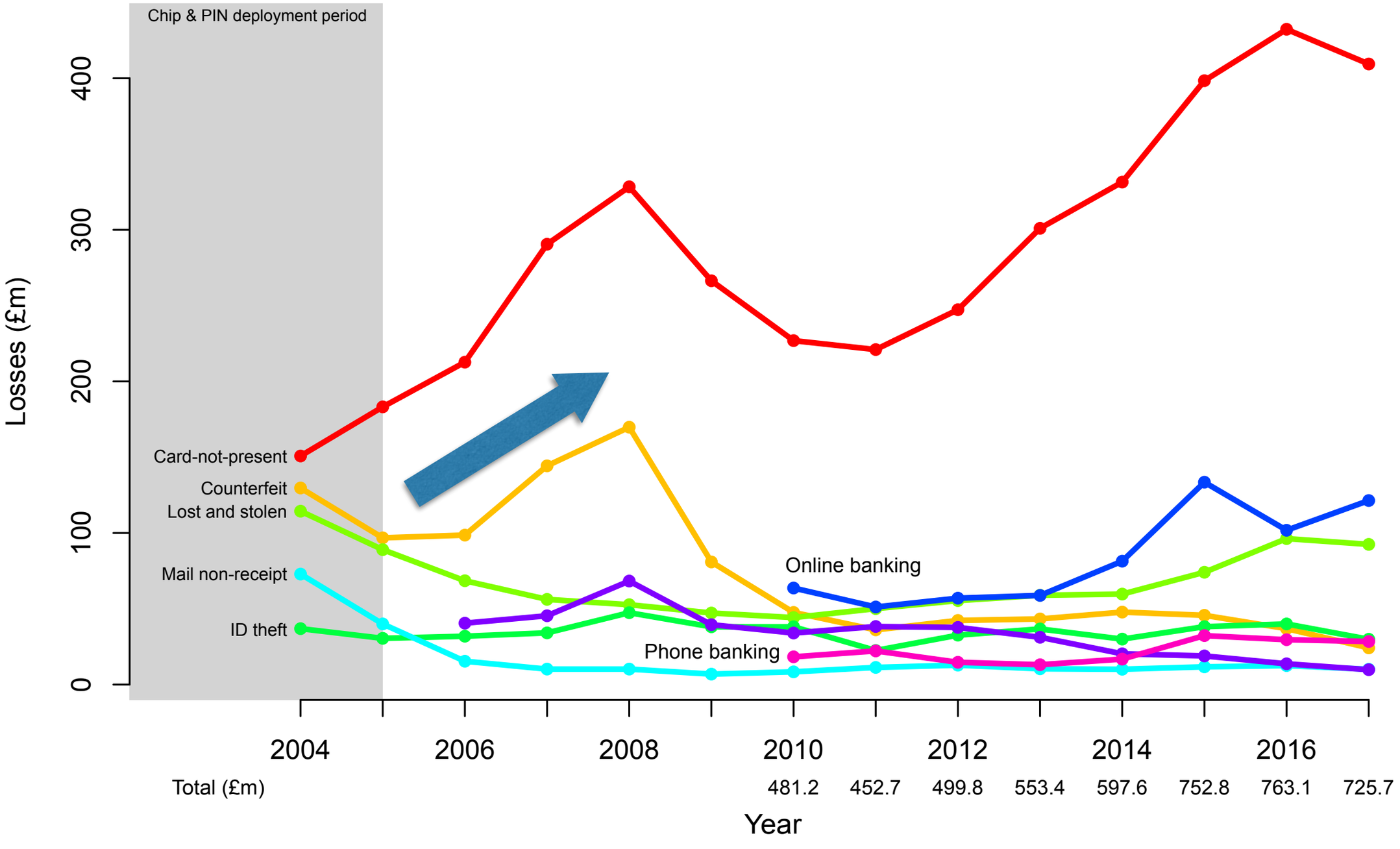
Cardholder verification



Transaction authorisation

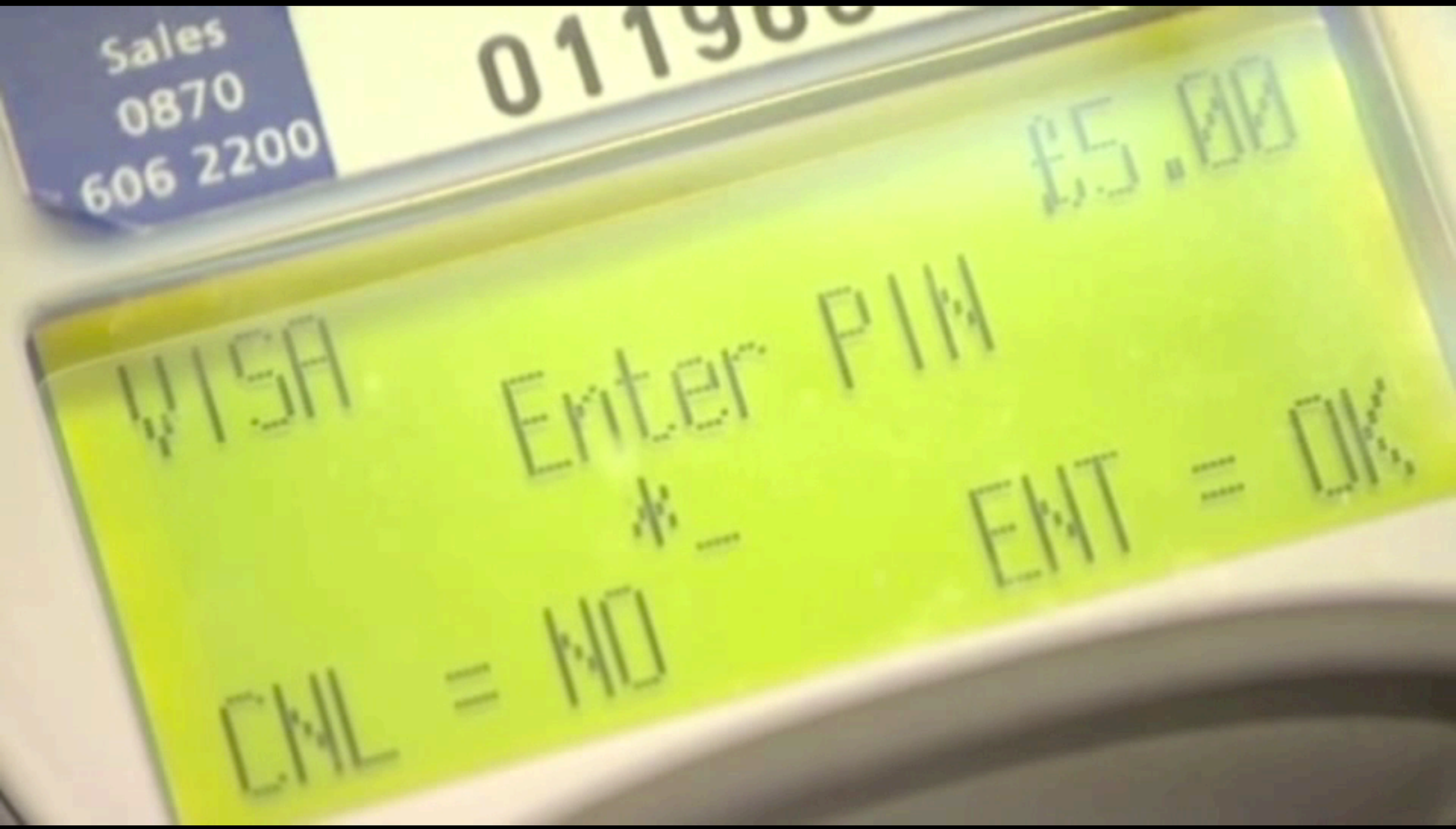


Chip and PIN led to increase in counterfeit fraud

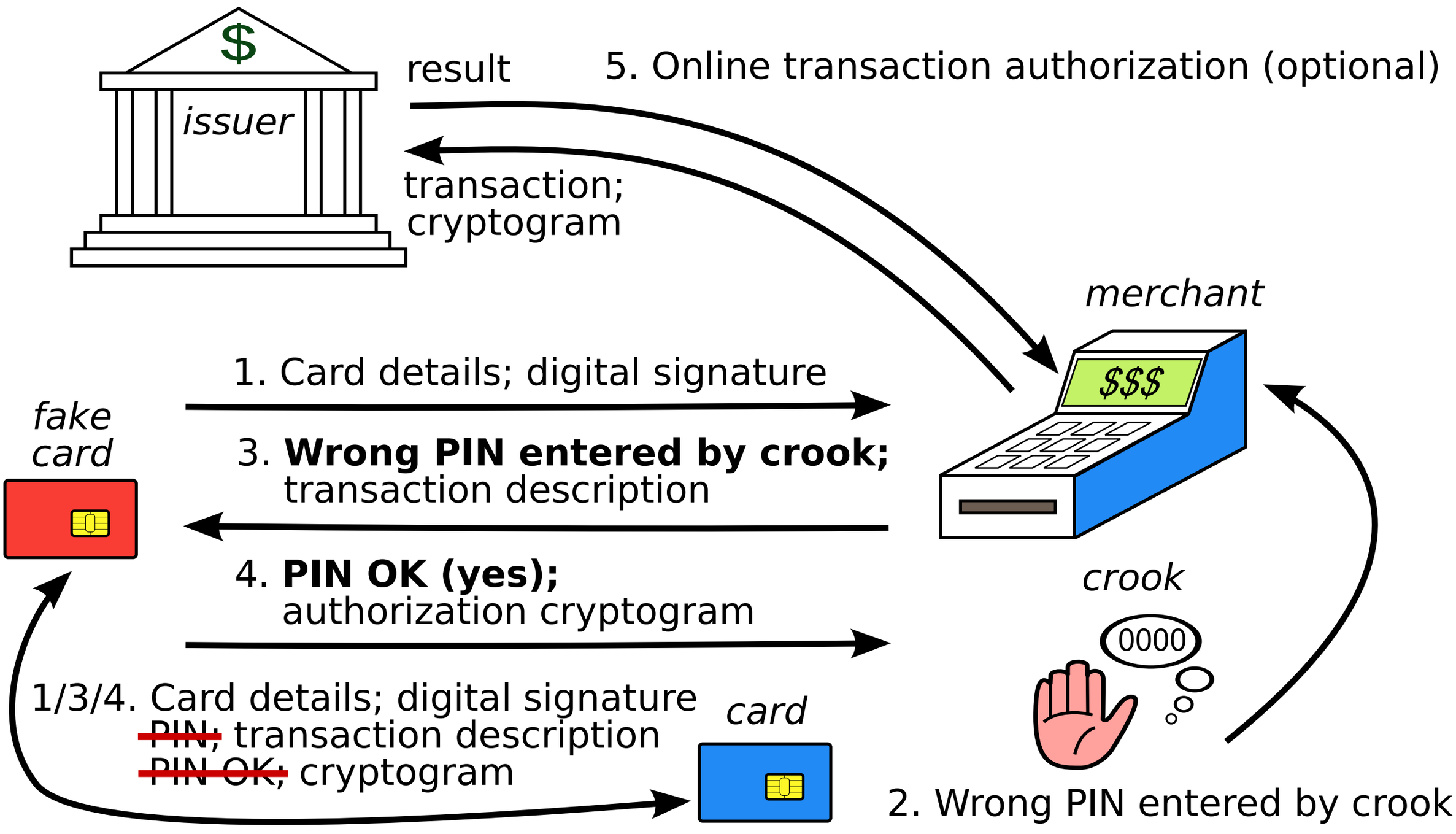


Card is responsible for cardholder verification

- Card states ways by which cardholder verification can be performed and the preference (e.g. first PIN, then signature)
- If PIN used, terminal sends PIN to card and card checks if correct
- PIN sometimes encrypted
- Response **not encrypted or authenticated**


Sales
0870
606 2200
WISA
Enter PIN
£5.00
CNL = NO
ENT = OK

The no-PIN attack



Response from industry

> What is more, at this stage, the observations are the result of scientific research whose transposition outside laboratory conditions is complex since it would necessitate the use of highly sophisticated material.
>
> — Le GIE des Cartes Bancaires (January 2010)

> Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks.
>
> — UK Cards Association (February 2010)

UK Cards Association (1 year after disclosure)

"It is the publication of this level of detail which we believe breaches the boundary of responsible disclosure. Essentially, it places in the public domain a blueprint for building a device which purports to exploit a loophole in the security of chip and PIN.

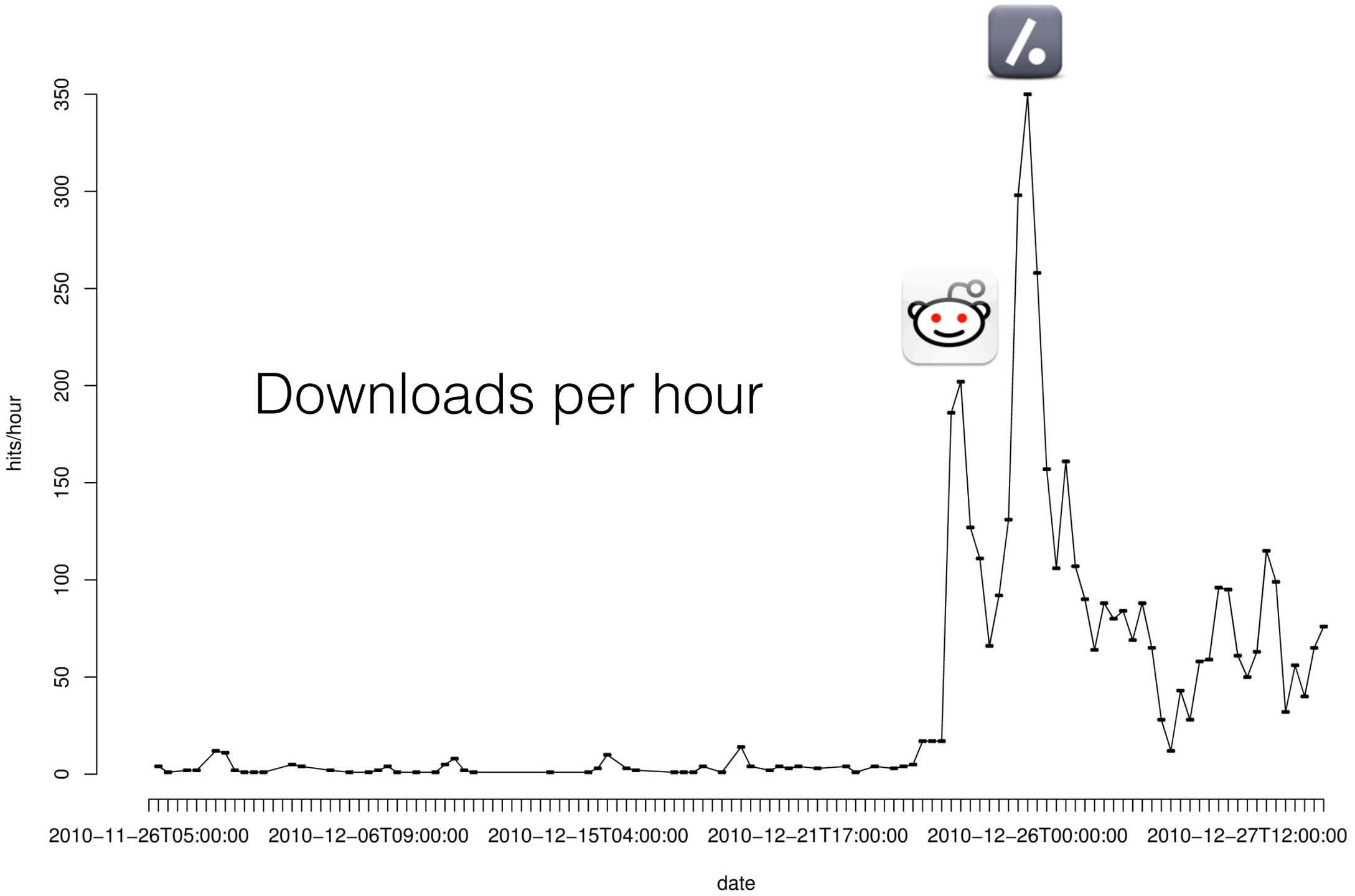
...

Consequently, we would ask that this research be removed from public access immediately and would hope that you are able to give us comfort about your policy towards future disclosures."

Ross Anderson responds

"Second, you seem to think that we might censor a student's thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Erasmus, of Newton, and of Darwin; censoring writings that offend the powerful is offensive to our deepest values."

The Internet



Criminals (2 years after disclosure)

The unstoppable credit card scam

A device to neutralize the security chip bank card was used for the first time in France. Many scammers have been arrested, but this scam still does not have a parade.

Published on 24.01.2012

Crooks, highly experienced, have managed to bypass the security chip embedded bank cards - deemed inviolable - before multiplying scams. The technique - unearthed in 2010 by a British academic, Professor Ross Anderson - was applied for the first time in France by a team based in the Paris region and in the north. Many of them have just been arrested by investigators from the Central Office for the Fight against crime related to information technology and communication (OCLCTIC). According to preliminary investigation, the thugs have made nearly 6,000 purchases for damages of more than € 500,000. Officers fear that this technique spread. "For the time being, even if the person who was stolen or lost card opposed to the latter, scammers may nevertheless continue to use it, says a specialist officer. That's the whole problem with this scam. Thieves rajoutent on the map stolen a second chip that tricks the payment terminal at the merchant, into believing that the PIN is the correct compound. The

ON THIS TOPIC

Do you trust your credit card?

NEWS FLASH LAST MINUTE

0:07 Spain: first hitch for Barca, Sevilla co-leader
11:41 p.m. Italy: AS Roma clings
23:05 Germany: Leverkusen back, Dortmund stalled
10:48 p.m. Hand: Dunkirk relapse, PSG wakes
10:29 p.m. Nigeria: Army says the head of Boko Haram died
9:55 p.m. Death of Gérard Violette, director of the Historic City Theatre
9:22 p.m. Ligue 1: Paris recovers, gives Lille, Monaco connects

ALL NEWS

MORE ARTICLES ...

VIEWED COMMENTED SHARED

9/24/2014 9:43 p.m. at the
Algeria: French hostage Hervé Gourdel was executed by jihadists

9/24/2014 7:11 in the
station: a drink, sanctions ... and a strike

9/25/2014 0:06 in the
Death of French hostage: "Authors should be punished," warns Holande

HOW DOES THE STRATEGY WORK

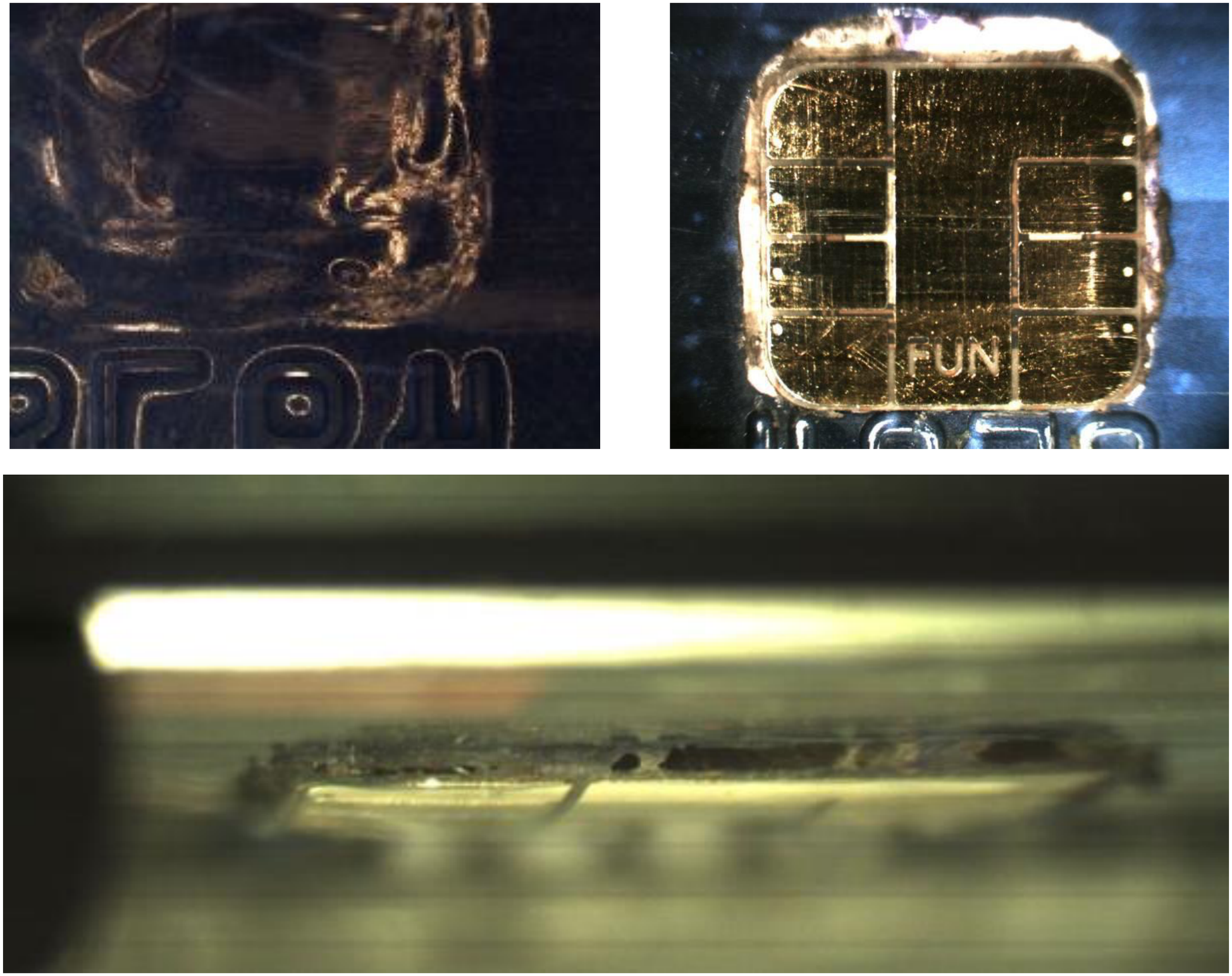
1 Scammers **steal bank cards by stealth** to avoid attracting the attention of their victims too quickly.

2 They then modify the card, replacing **existing chip with another,** programmed with **soft-ware that blocks the security**

3 The scammers can then **enter any PIN** to pay for purchases costing less than €100.

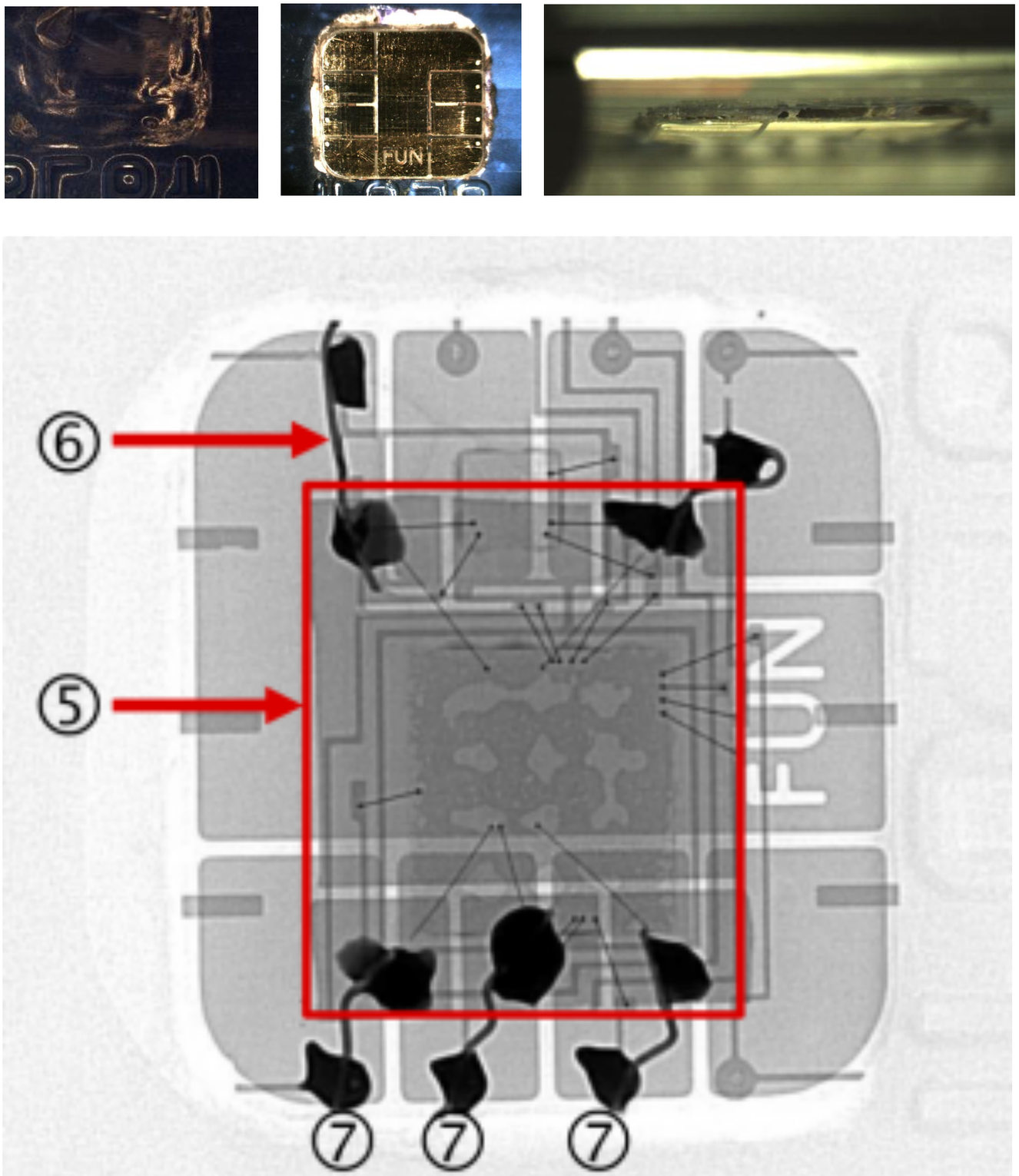
4 The scammers are buying, in general, **consumer products that can be quickly sold** on black-market.

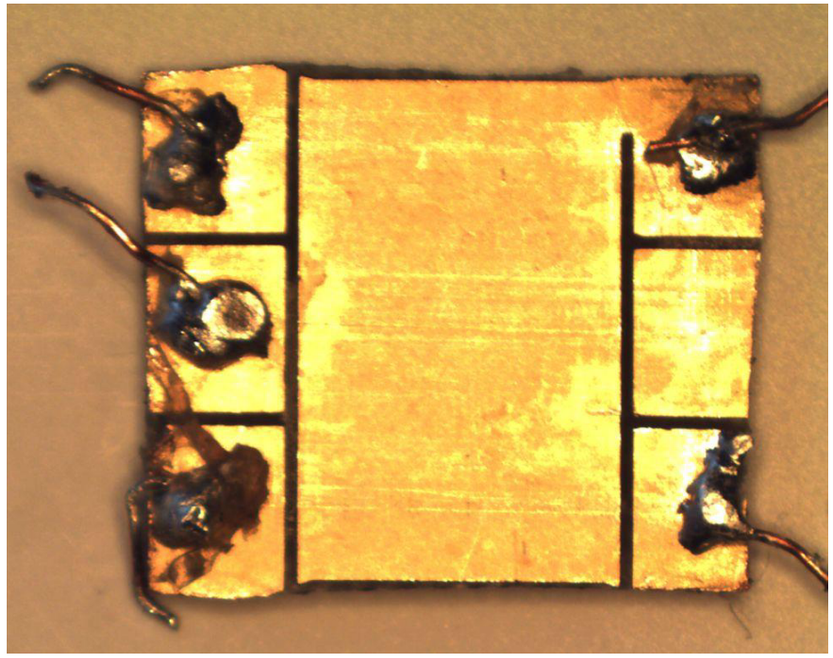
Response from criminals

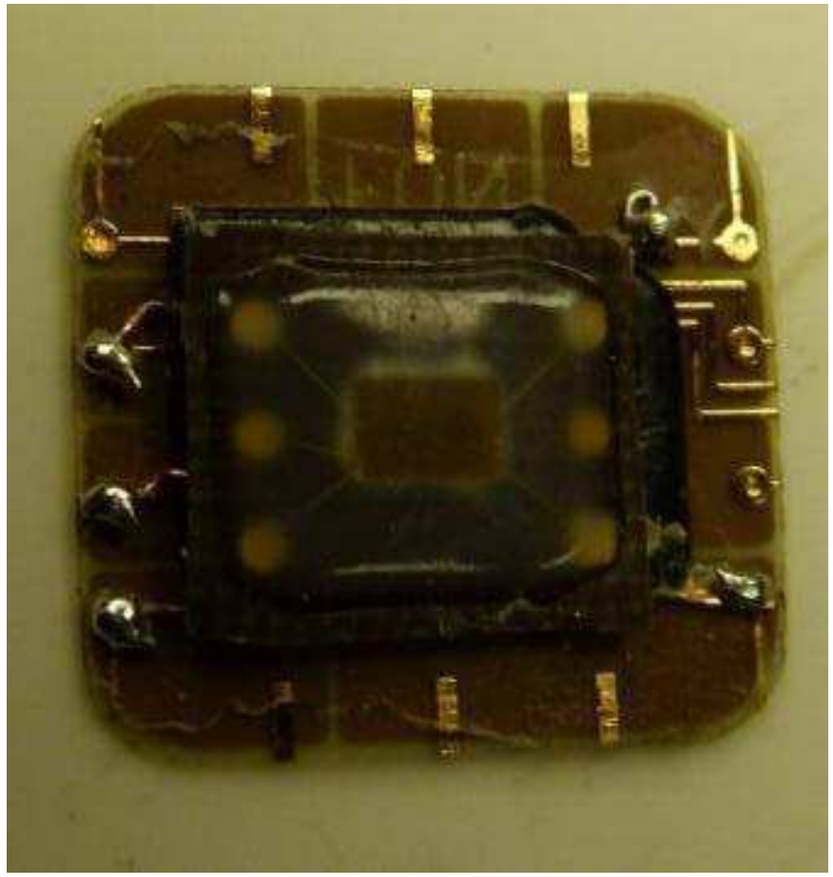


Ferradi et al. “When Organized Crime Applies Academic Results – A Forensic Analysis of an In-Card Listening Device”, Cryptology ePrint Archive: Report 2015/963.

Response from criminals







Ferradi et al. “When Organized Crime Applies Academic Results – A Forensic Analysis of an In-Card Listening Device”, Cryptology ePrint Archive: Report 2015/963.

Pay a bill

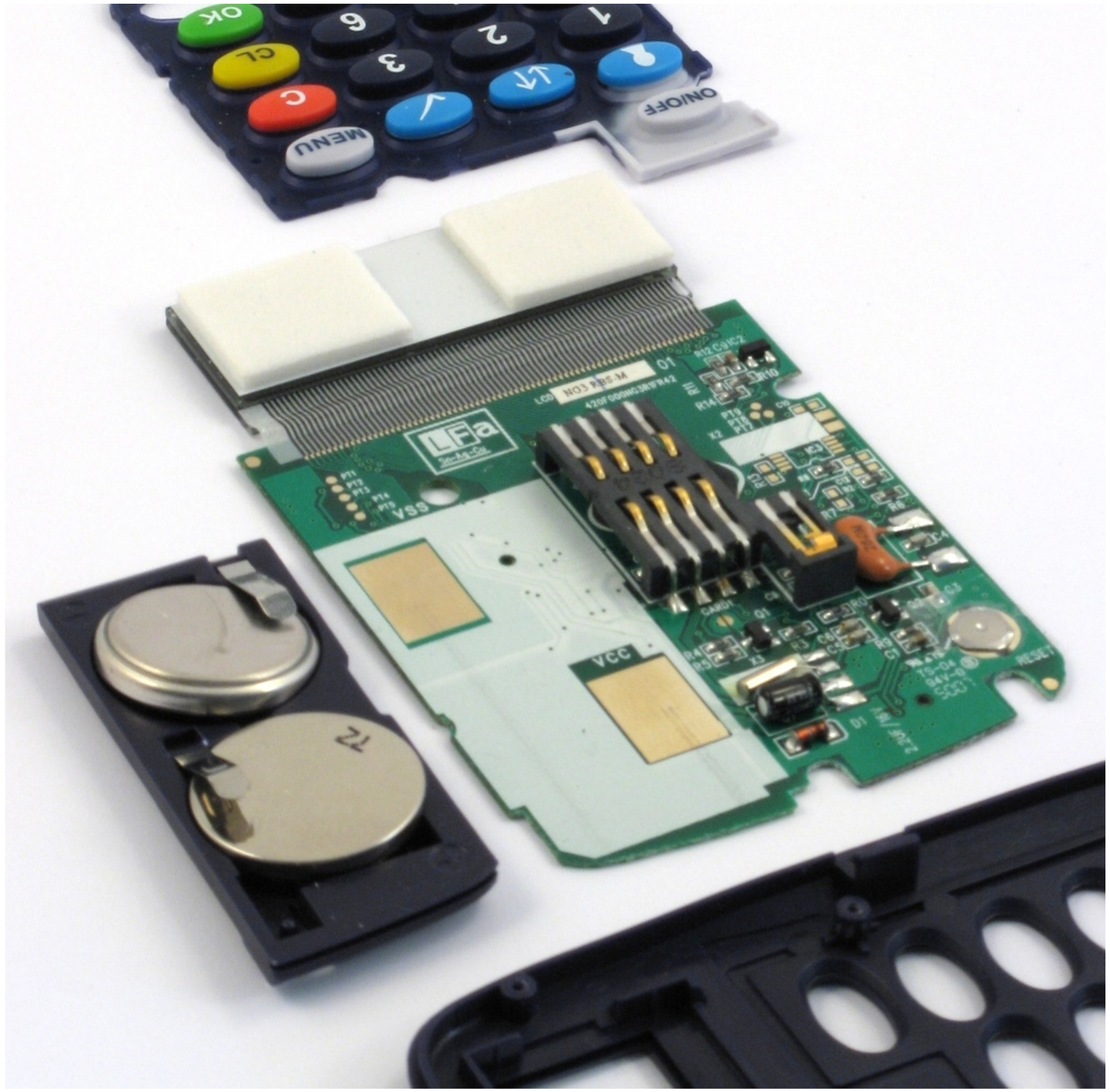
Destination account number

Recipient name

Amount

One time password

EMV-CAP in the UK



EMV CAP's weakness: attacker controls user experience

- User thinks they are typing random challenge but it is really part of an account number

- User thinks it's OK that details on device don't match those they entered on the computer

- User thinks they are performing a POS transaction but really it's online banking

Usability is a security requirement

If something goes wrong do you get your money back?

- In the US, very likely yes (Regulation E & Z)

- In the EU, it's more complicated (Payment Services Directive) …

- Banks are permitted to refuse a refund for unauthorised transaction if customer was "grossly negligent" in complying with bank terms and conditions

- What is considered "grossly negligent" and is this definition fair?

Example T&C (HSBC UK)

"You must take **all reasonable precautions … including** but are not limited to:

…

not choosing security details that may be **easy to guess**

…

Never writing down or otherwise recording your PIN and other security details in a way that can be understood by someone else

…

keeping your security details **unique to your accounts with us**

…

not allowing anyone else to have or use your card, security devices, PINs, or any of your security details"

Over 1/3 of customers have 3 or more PINs

	0	1	2	3	4	5	6	7	8	9	mean
4 digits	1	88	65	41	31	8	5	1	1	0	2.28
5 digits	233	5	3	0	0	0	0	0	0	0	0.05
6 digits	228	8	4	1	0	0	0	0	0	0	0.08

Almost half of PINs are used once per month or less frequently

	4-digit PINs								
	#1	#2	#3	#4	#5	#6	#7	#8	Sum
Every day	34	0	0	1	0	0	0	0	35
Several times a week	117	30	3	3	0	0	0	1	154
Once per week	59	35	12	3	0	0	0	0	109
Once per month	21	37	24	8	3	0	0	0	93
Several times per year	6	24	24	12	2	2	1	0	71
Once per year or less	1	14	10	10	4	1	0	0	40
Never	2	12	14	9	6	4	1	0	48

Customers find ways to manage this otherwise impossible task

- About 1/3 of customers write down their PIN and keep it with the card (e.g. in a wallet, diary, phone)

- About 1/4 of customers use their PIN elsewhere (mainly mobile phone)

- About 1/2 of customers share their PIN with someone else (mainly spouse/partner or other family members)

- **These actions are treated as gross negligence if there is no other more likely explanation for fraud**

- Is this fair? What can be done about it?

BBC

A loophole in Payment Services Directive shifts liability for push payment fraud

- Customer is not liable unless bank believes customer is negligent

- However this criteria only applies for unauthorised transactions

- UK banks claim that if you perform an action that leads to a transaction being performed then you have “authorised” that transaction

    - Even if you intended something else to happen

- Voluntary code of conduct is being developed

Conclusions

- The need for threat modelling differentiates security engineering from systems engineering

- Verifying a protocol to be secure is challenging but is possible to do

  - Security is only with respect to a model, and the model might not match reality exactly

- Economics and usability play as much a role within security engineering as cryptography

More information

THE CONVERSATION

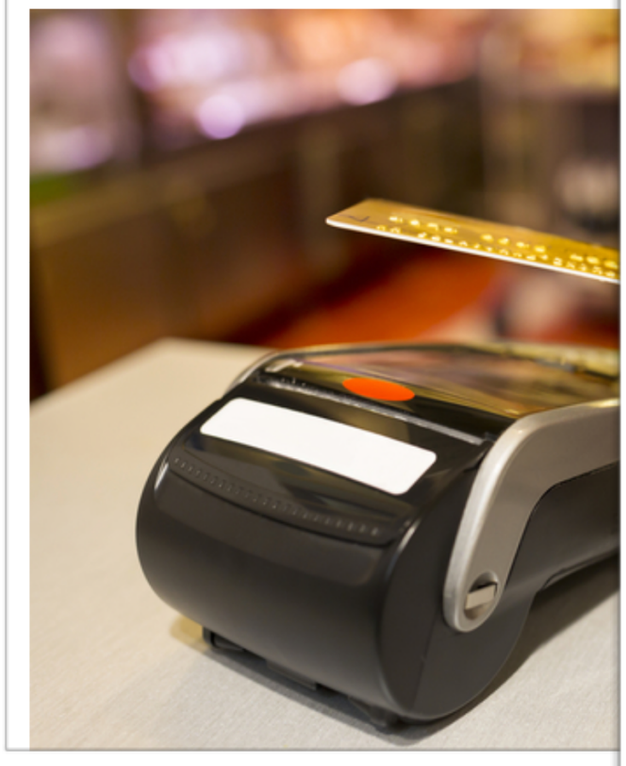
Academic rigour, journalistic flair

Search analysis, research, academics…

Arts + Culture | Business + Economy | Education | Environment + Energy | Health + Medicine | Politics + Society | Science + Technology | Rugby World Cup

Banks undermine chi
because they see pro
than fraud

March 30, 2015 12.20pm BST



Bentham's Gaze

Information Security
Research & Education,
University College London

About this site

Information Security
Research Group @ UCL

ACE-CSR @ UCL

MSc Information Security

Contribution policy

Search …

Just how sophisticated will card fraud techniques become?

In late 2009, my colleagues and I discovered a serious vulnerability in EMV, the most widely used standard for smart card payments, known as “Chip and PIN” in the UK. We showed that it was possible for criminals to use a stolen credit or debit card without knowing the PIN, by tricking the terminal into thinking that any PIN is correct. We gave the banking industry advance notice of our discovery in early December 2009, to give them time to fix the problem before we published our research. After this period ex-

https://www.benthamsgaze.org/