Payment system governance – security economics at large

Ross Anderson
Cambridge

Payment Systems

- Early modern period: merchant bankers carried risks of financing trade
- 19th century: industrialised by letters of credit, insurance certificates, bills of lading, inspection certificates, the telegraph
- People could do business with remote merchants
- Late 20th century: the Internet and credit cards
- Would the banks earn lots as the trust provider?

A Natural Experiment

- Stronger US consumer protection
  - Judd v Citibank 1980
  - Reg E
- Weaker UK consumer protection
  - McConville et al v Barclays et al 1993
  - Banking code, Financial Ombudsman Service
- Other countries spread out: F, De, E, ZA …
- Payment Services Directive trying to harmonise
- Some system issues becoming clear

EMV (‘Chip and PIN’)

VISA

EXP: 30/11/09 ICC

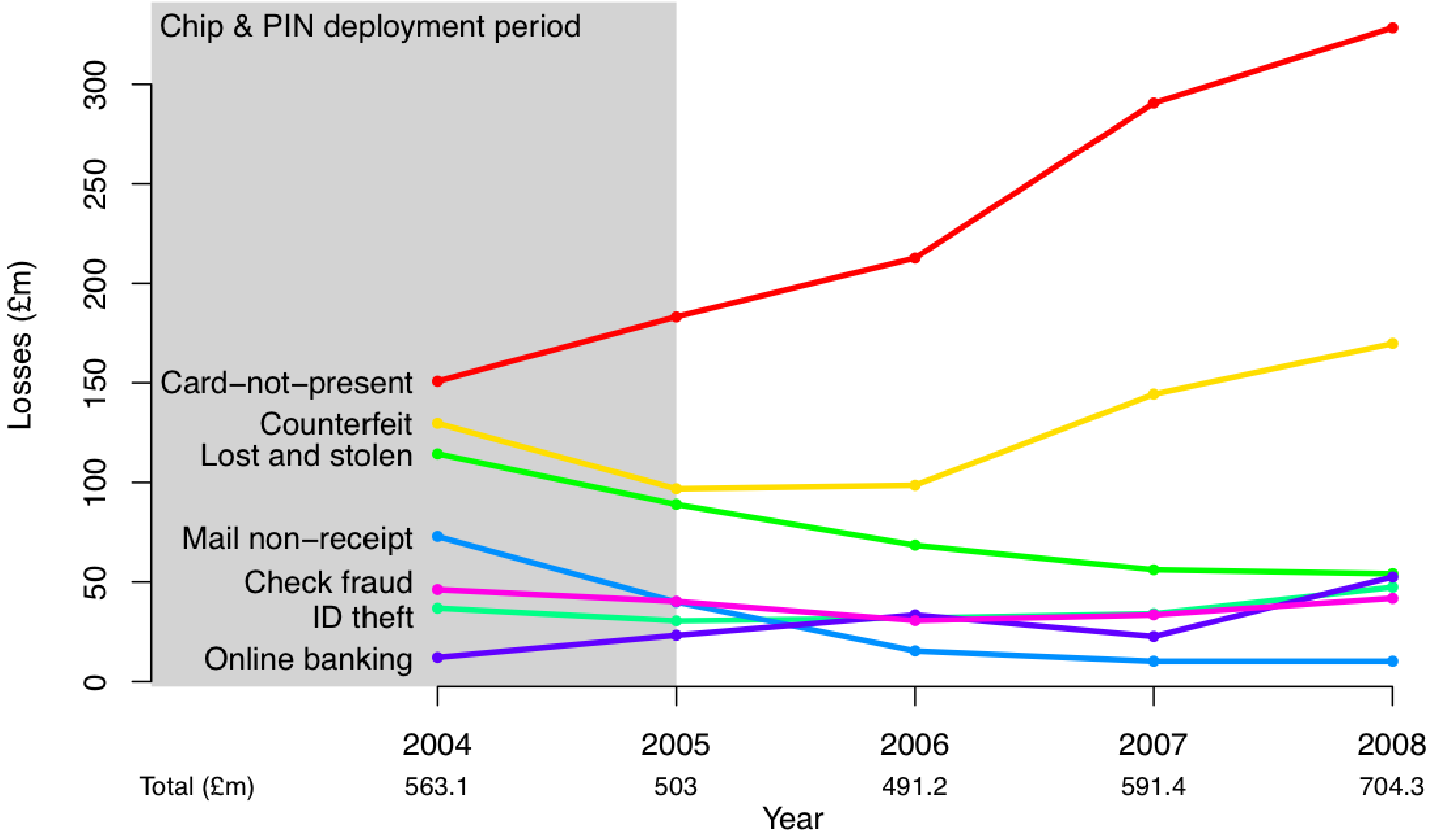
SALE

£50.00

VERIFIED BY PIN

- Now deployed in Europe and elsewhere
- ‘Liability shift’ – disputes charged to cardholder if pin used, else to merchant
- Changed many things, not always in the ways banks expected!

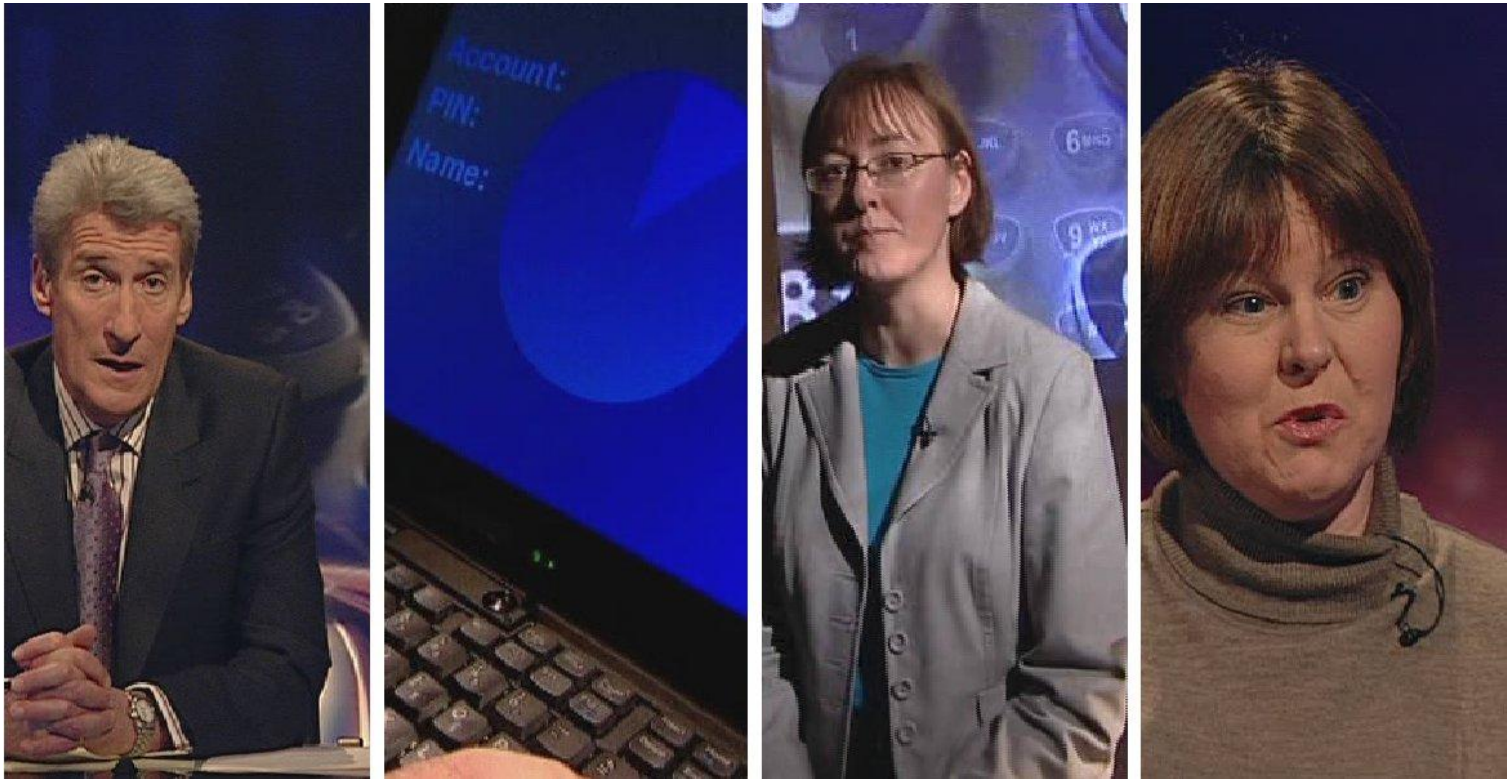
Fraud in the UK since EMV



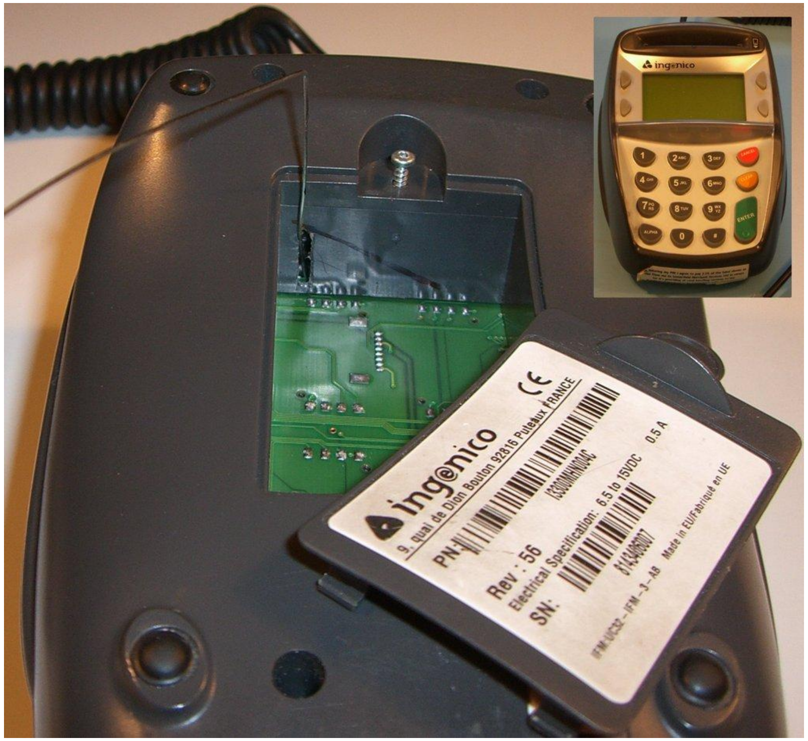
Tamper-proofing of the PED

- In EMV, PIN sent from PIN Entry Device (PED) to card
- Card data flow the other way
- PED supposed to be tamper resistant according to VISA, APACS (UK banks), PCI
- Evaluations follow Common Criteria
- Should cost $25,000 per PED to defeat

Exposed on TV (Feb 26 2008)

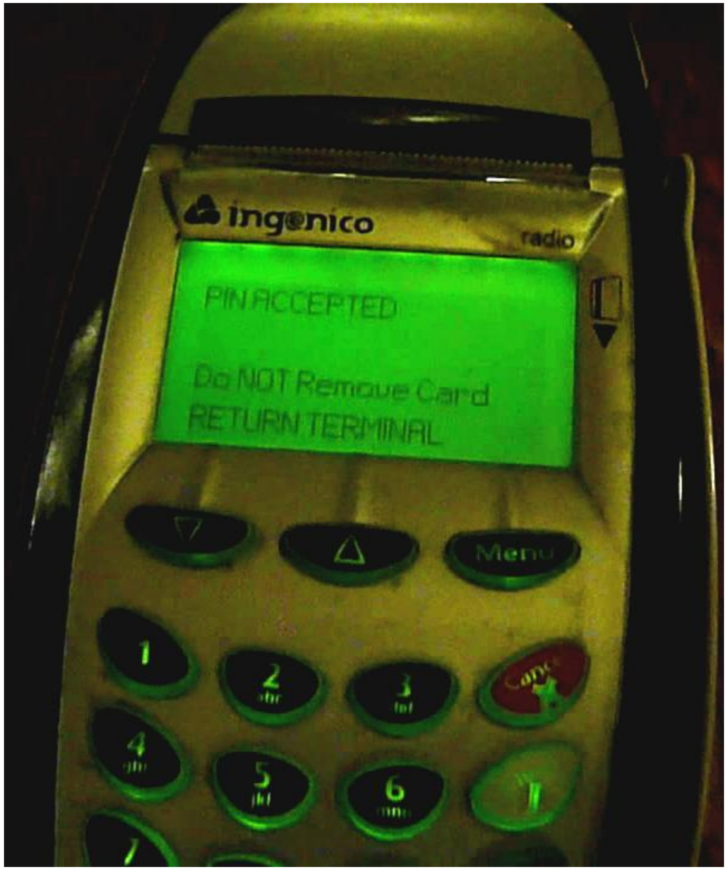


Security economics


ingenico
ingenico
9, quai de Dion Bouton 92816 Puteaux FRANCE
PN
Rev : 56
Electrical Specification: 6.5 to 15VDC 0.5A
SN:
Made in EU/Fabriqué en UE
ENTER

- Acquirers and issuers have different incentives
- PEDs ‘evaluated under the Common Criteria’ were trivial to tap
- Banks said in Feb 08 it wasn’t a problem…
- By July 2008 we saw tampered PEDs coming from the factory!

The ‘No PIN’ attack

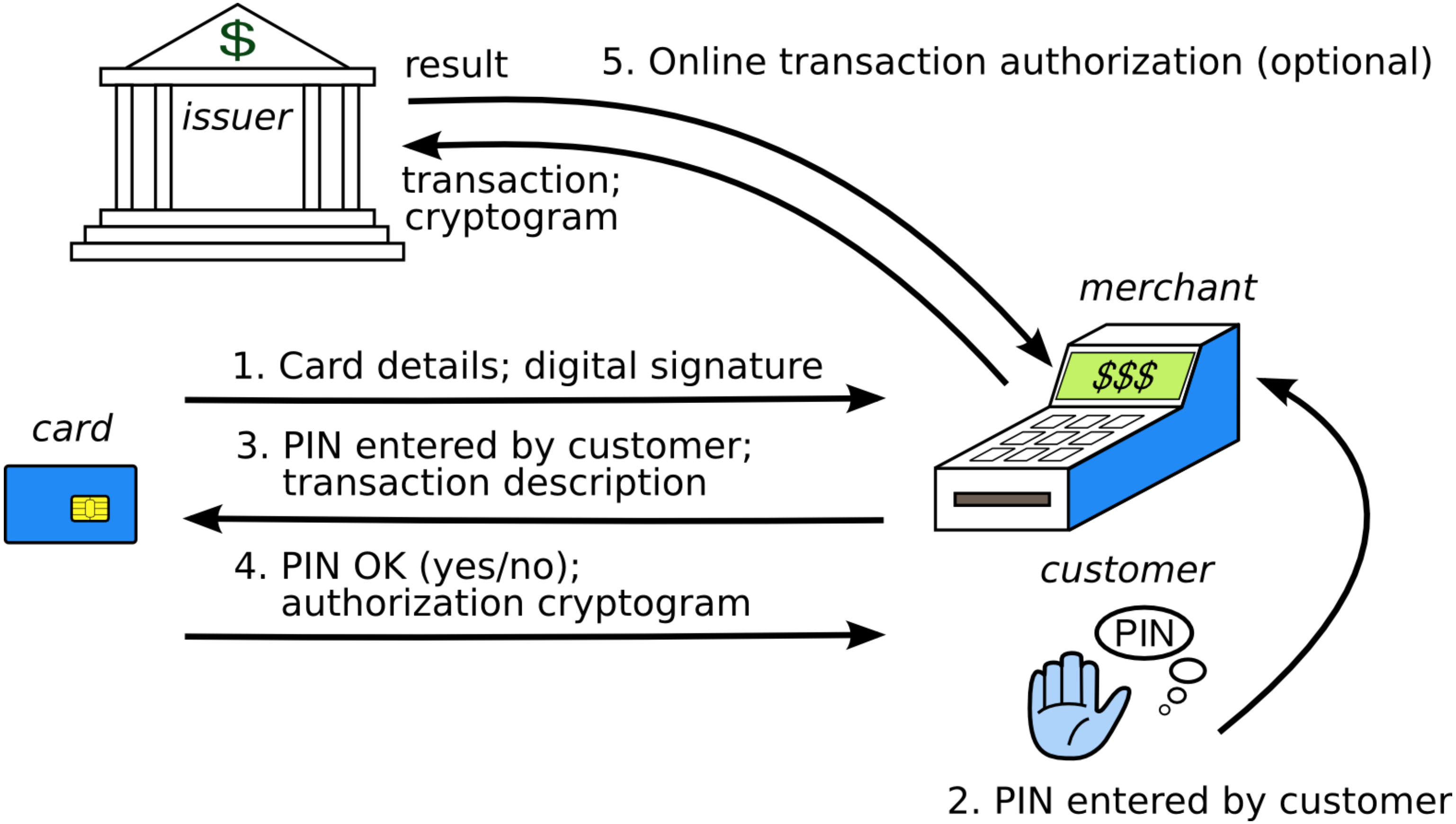


- This attack lets crooks use a stolen card without knowing the pin
- We insert a device between card & terminal
- Card thinks: signature; terminal thinks: pin
- Works even for online transactions (and DDA)

Exposed on TV

Newsnight, BBC2, Feb 11 2010

A normal EMV transaction



result

5. Online transaction authorization (optional)

transaction;
cryptogram

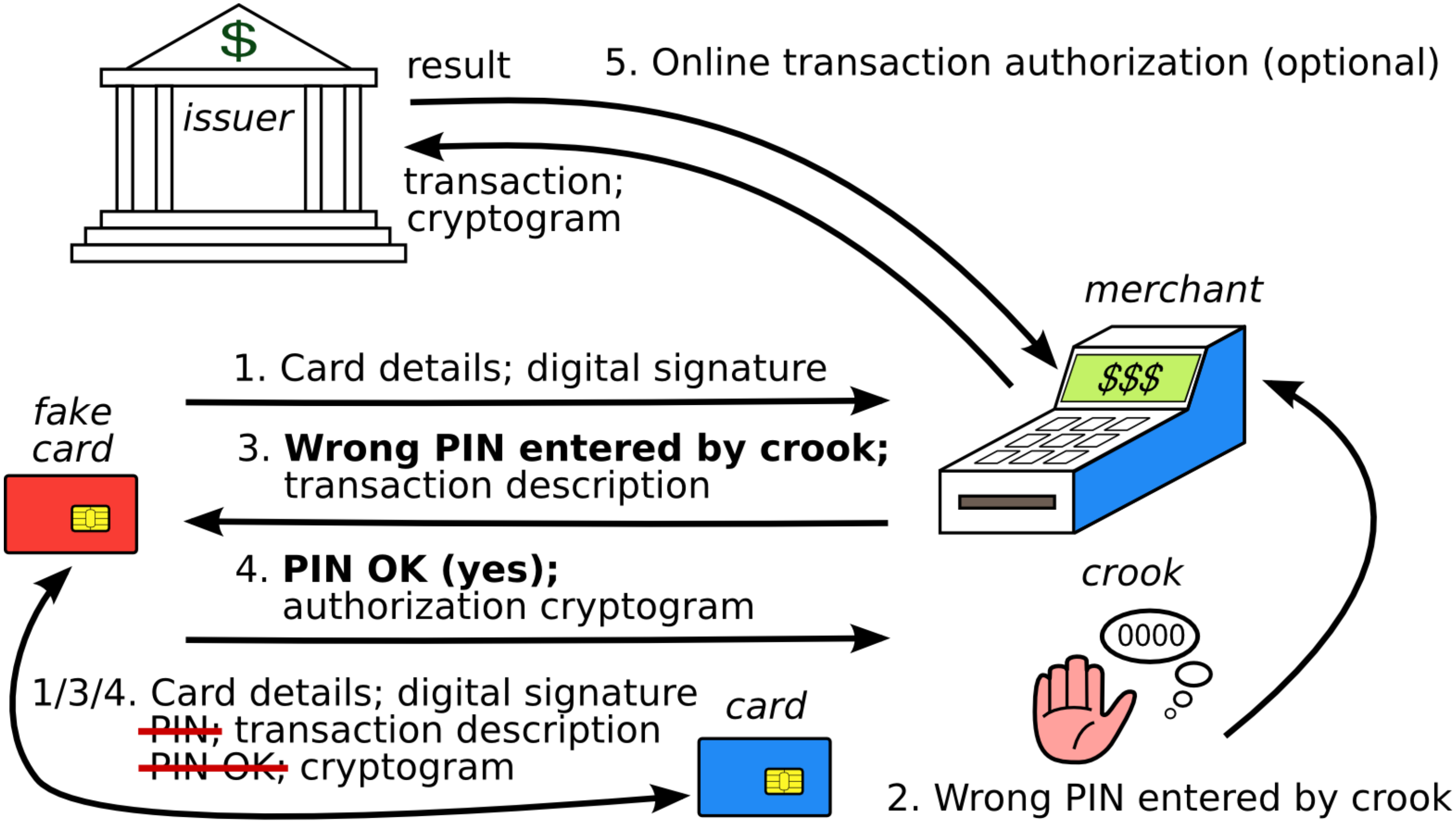
1. Card details; digital signature

3. PIN entered by customer;
transaction description

4. PIN OK (yes/no);
authorization cryptogram

2. PIN entered by customer

A ‘No-PIN’ transaction



result

5. Online transaction authorization (optional)

transaction;
cryptogram

1. Card details; digital signature

3. **Wrong PIN entered by crook;**
transaction description

4. **PIN OK (yes);**
authorization cryptogram

1/3/4. Card details; digital signature
~~PIN;~~ transaction description
~~PIN OK;~~ cryptogram

2. Wrong PIN entered by crook

Blocking the ‘No PIN’ attack

- The card tells the issuer ‘signature used’ while the terminal tells the acquirer ‘pin used’
- In theory: might block at terminal, acquirer, issuer
- In practice: may have to be the issuer (as with terminal tampering, acquirer incentives are poor)
- Tactical problem: messages get mangled!
- Real problem: EMV spec now vastly too complex
- With 100+ vendors, 20,000 banks, millions of merchants … a tragedy of the commons

Regulators and Fraud

- Regulators were too ready to believe bank assurances about credit risk management
- There is a similar problem with operational security risk management
- Wherever regulators let them, banks are dumping the risk of fraud on customers – merchants and cardholders – and even on each other
- This is starting to create systemic risk
- What’s the optimal regulatory approach?

Payment research topics?

- Interesting case histories?
  - Korean online banking, CAP, proceeds of crime , …
- How to align incentives, foster innovation?
  - Cap interchange fees?
  - Do something about compliance costs?
  - Level the playing field for paypal, facebook,…?
  - Open standards?
  - Managed upgrade cycle for noncompetitive platforms?
  - Other governance routes?