Secure Payments in the Electronic World

Banking, financial technology, and security awareness
11/12 December 2004

Chris Mitchell
Information Security Group
Royal Holloway, University of London
http://www.isg.rhul.ac.uk/~cjm

Contents

1 Risks and requirements in the Electronic World

Classical versus Electronic World I

Classical world

- Traditional players
- Bank controlled networks
- Physical presence of cardholder
- physical authentication characteristics of the card
- comparison of signature
- two card technologies

Electronic world

- New players (e.g. MSPs)
- Networks not controlled by banks
- Unprotected transmission of data
- payment and personal details
- physical characteristics of card can no longer be used

Classical versus Electronic World II

Classical world

- Physical presence of merchant
- physical presence at store of goods that can be seen and touched
- delivery of goods against payment

- Small scale

Electronic world

- Lack of human involvement
- more transactions
- more quickly and more cheaply

- Large scale
- in virtual world
- in other environments (cross-contamination)

Cardholder risks

- **Fraud scenarios**
  - Sites are created, collect payment data, and then disappear after fraudulently charging cardholders
  - Insecure (insufficiently protected) merchant servers
- **Main risks**
  - Transactions with fraudulent merchants
  - Debits for non-agreed service subscriptions
  - Transaction details stolen and re-used for another purpose (including cross-contamination)
  - Privacy violated

Merchant risks

- **Fraud risks**
  - Transactions with cardholders using stolen payment data, repudiated subsequently by legitimate owners
  - Cardholders falsely deny having ordered particular goods
  - Loss of confidentiality of transaction or consumer details
- **Business risks**
  - Investment in solutions that do not bring the expected revenue

Issuer and Acquirer risks

- **Common risk**
  - Increase in charge-backs and associated costs, in particular due to cardholder non-authorized transactions
- **Additional risks for issuer**
  - Cardholders not confident in payments in the Virtual World
  - Cardholder preference for other e- or m-payment security techniques
  - Merchants wait for implementation of security techniques

Formulating requirements

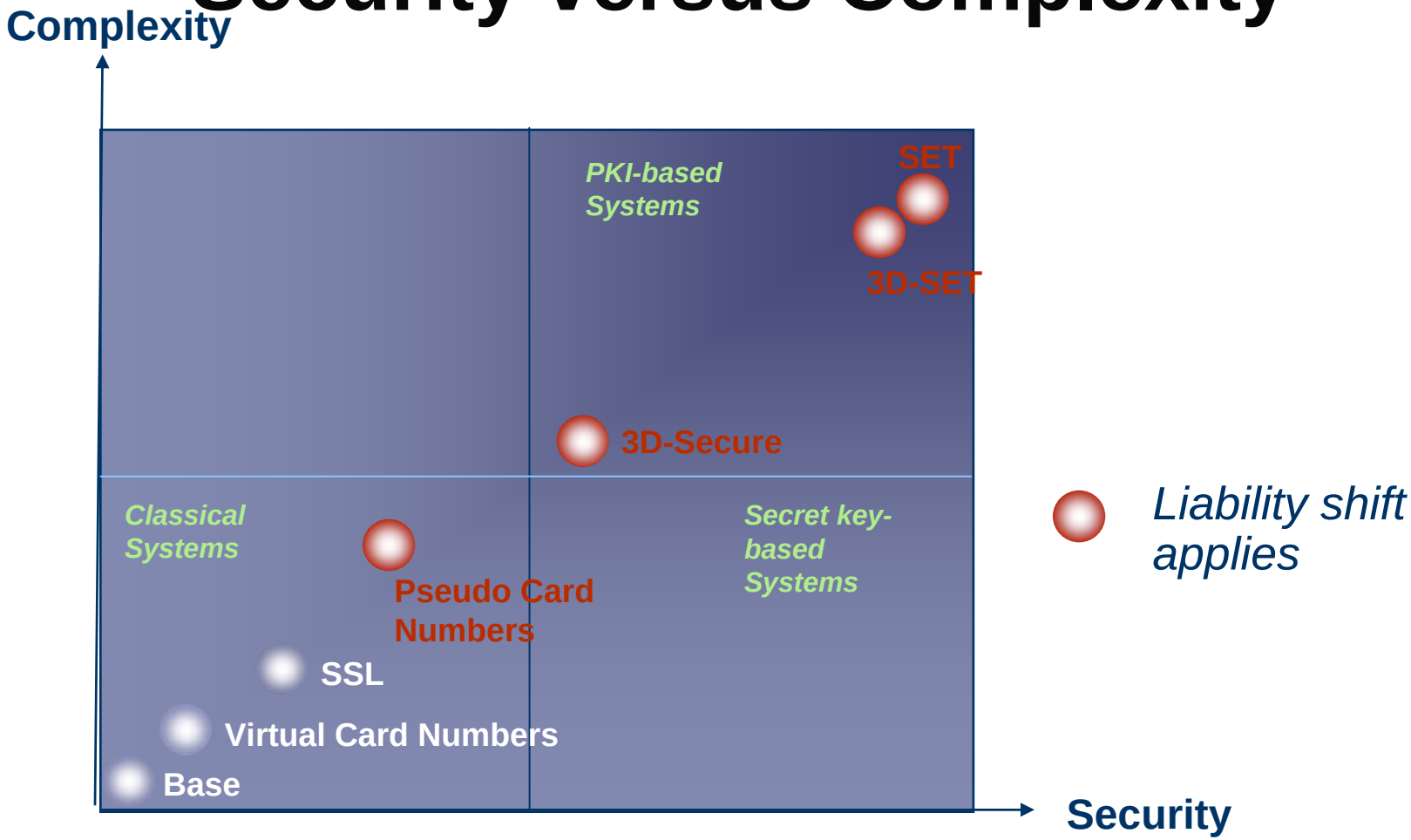
- **Security requirements**
  - Including confidentiality and integrity, merchant and cardholder authentication, and replay protection.
- **Business or personal requirements**
  - Including absence of liability in case of fraud, reduced charge-backs, etc.
- **Operational requirements**
  - Including ease of use/implementation, interoperability, device independence, etc.

2 Security Techniques for e-Payment

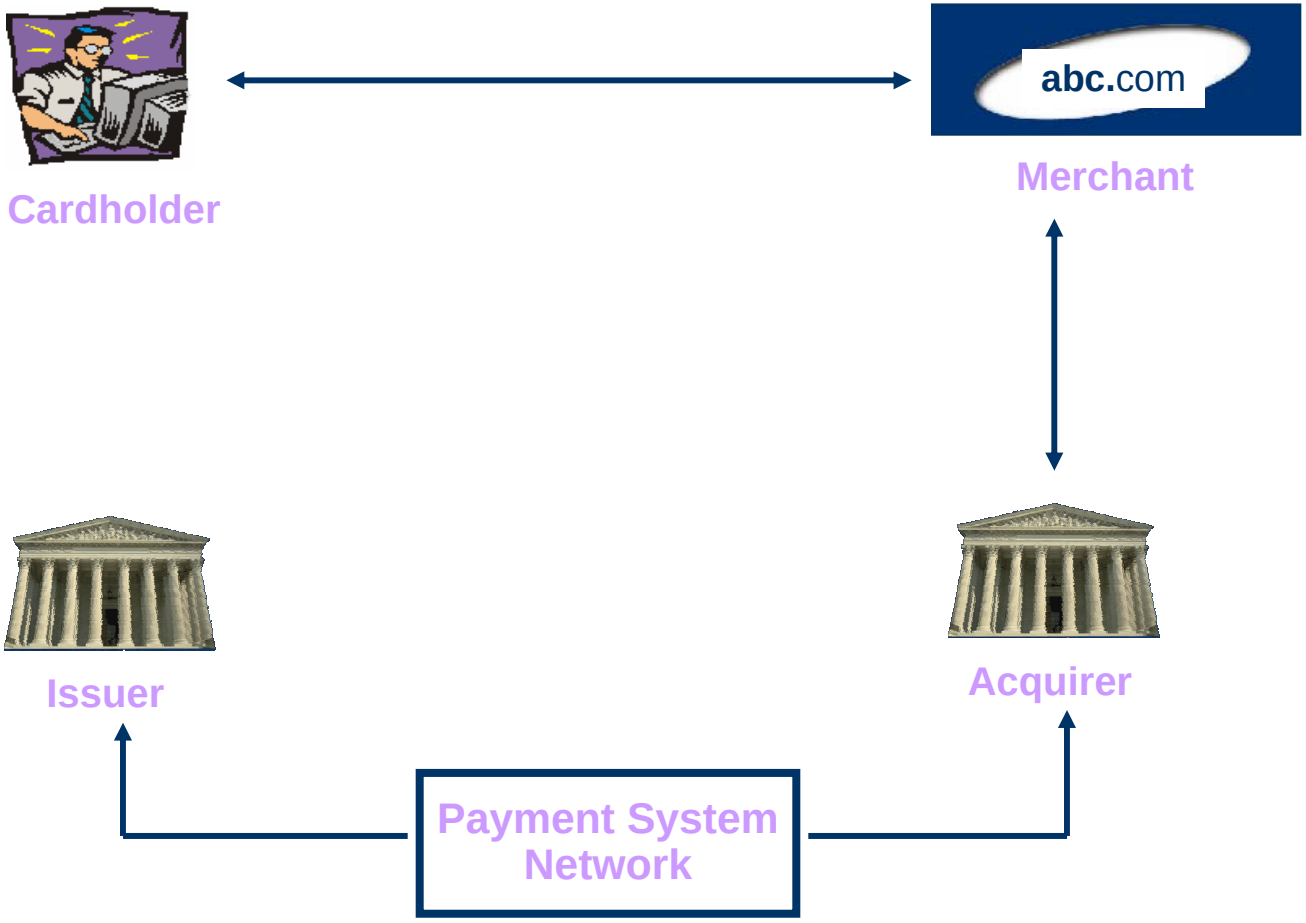
Liability shift

- **From security considerations**
  - Balance between added security and implementation cost/complexity
- **From business and operational considerations**
  - Merchant side of business no longer bears costs of fraudulent transactions
  - Issuers responsible for fraudulent transactions

Security versus Complexity



Early solution

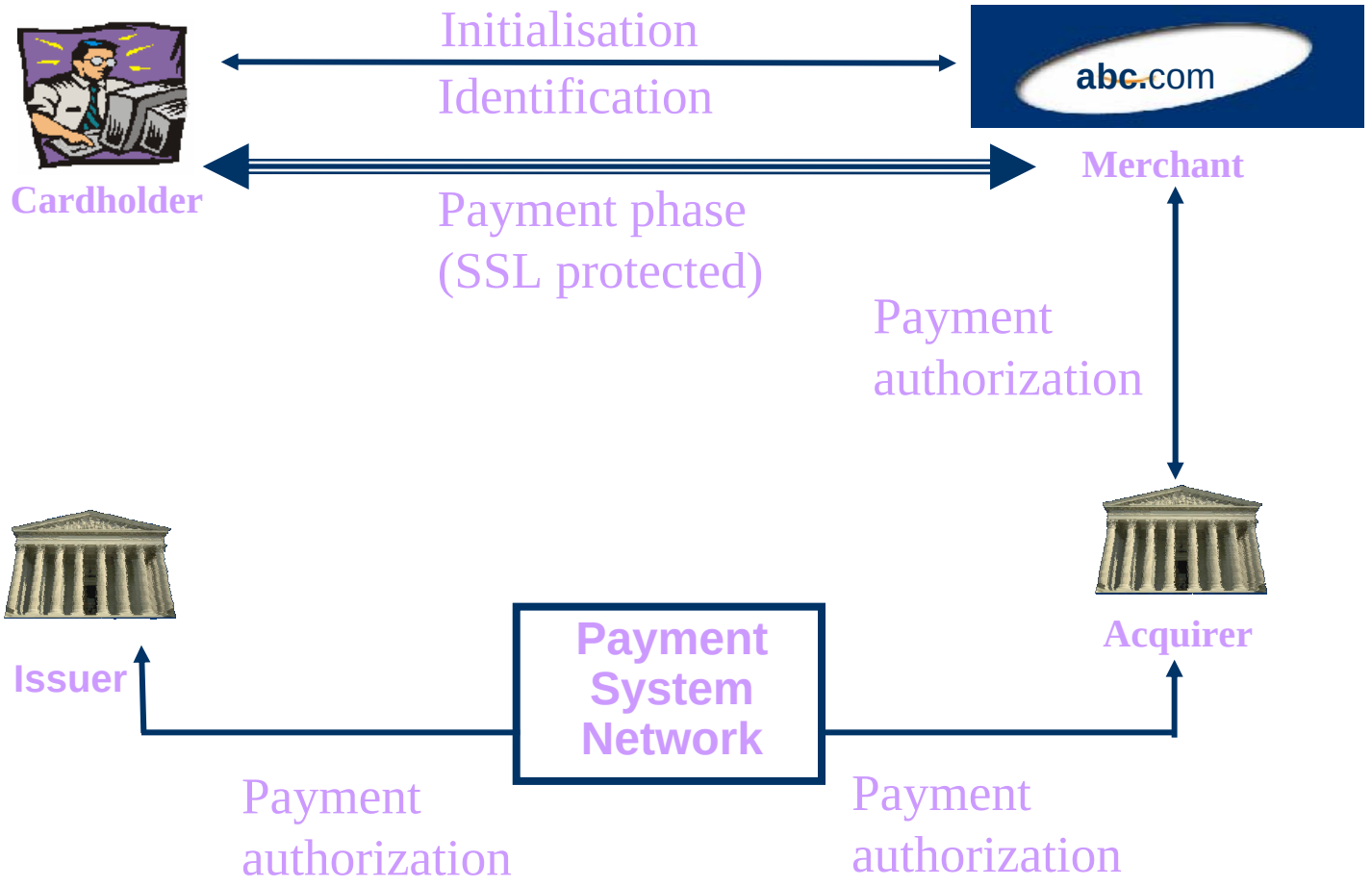


Early solution – analysis

- **Security considerations**
  - Absence of confidentiality, integrity, entity authentication, replay protection
  - Cardholder reluctance to provide card numbers
- **Operational considerations**
  - Ease of use and of implementation

Necessity to create new security techniques to manage the specific risks of payments in the electronic world

Secure Socket Layer (SSL)



Secure Socket Layer (SSL) – analysis

- **Security considerations**
- Protection of card details from hackers during transmission, using e.g. 128-bit algorithms
- Lack of protection of merchant databases from hackers
- Poor merchant identification and absence of cardholder authentication
- Attacks based on cardholder ignorance

- **Operational considerations**
- Ease of use and implementation

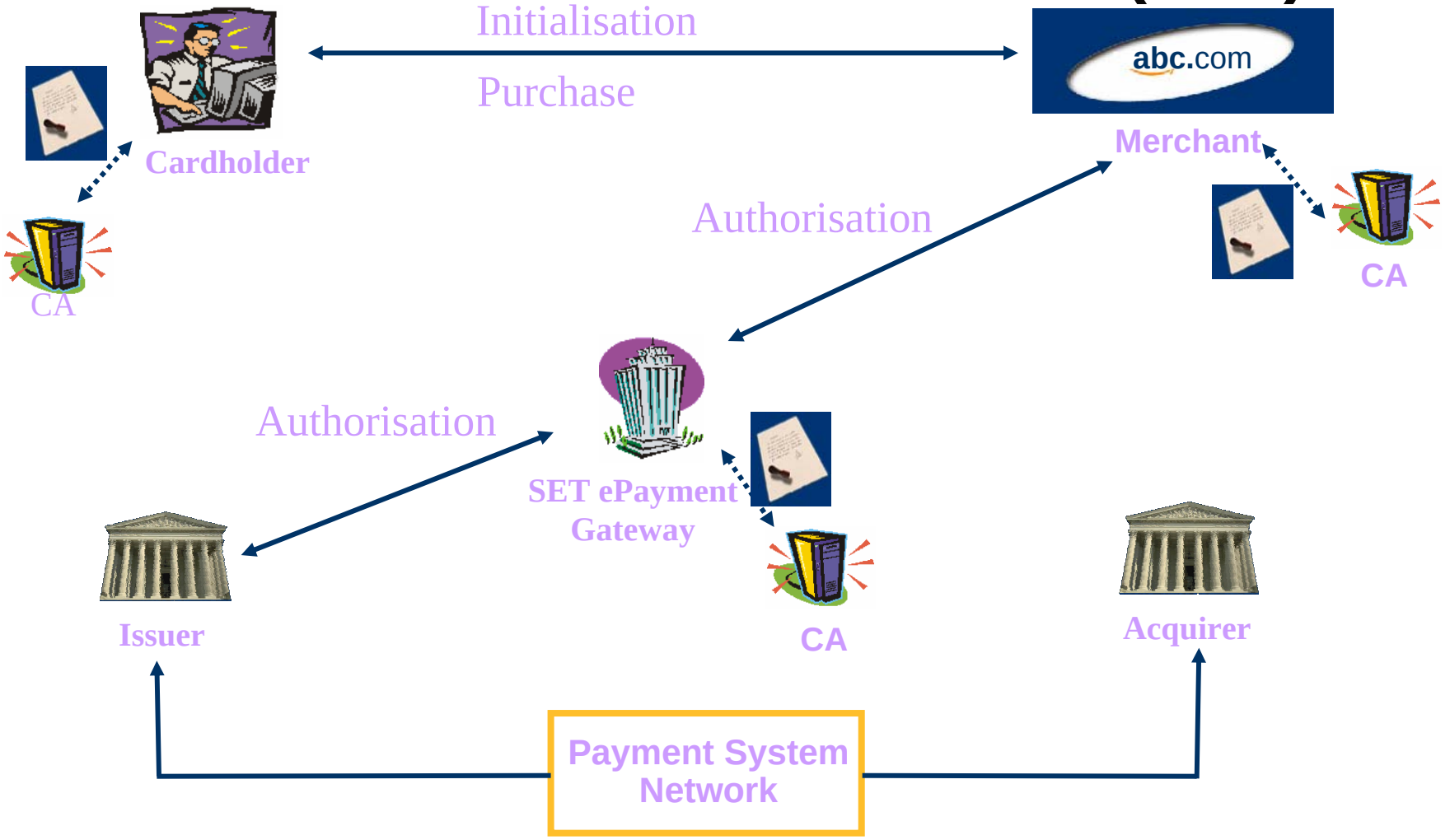
Virtual Card Numbers

- **Description**
- Static card numbers guaranteed for online purchases
  - used as stand-alone program
  - integrated into existing solutions (e.g. SSL)
- **Analysis**
- Prevention of cross-contamination
- No added complexity for cardholder
- No change on existing merchant infrastructure but high impact on issuer infrastructure
- Restricted Primary Account Number (PAN) space
- Hackers still able to conduct fraudulent Internet transactions

Pseudo Card Numbers

- **Description**
- Dynamic card numbers guaranteed for online purchases
  - expire quickly, depending on various criteria (transaction value, number of transactions, lifetime, etc.)
- Obtaining such numbers requires cardholder authentication
- **Analysis**
- Additional flexibility for cardholder but (low) added complexity
- No change in existing merchant infrastructure but high impact on issuer infrastructure
- Restricted Primary Account Number (PAN) space
- Liability shift applies

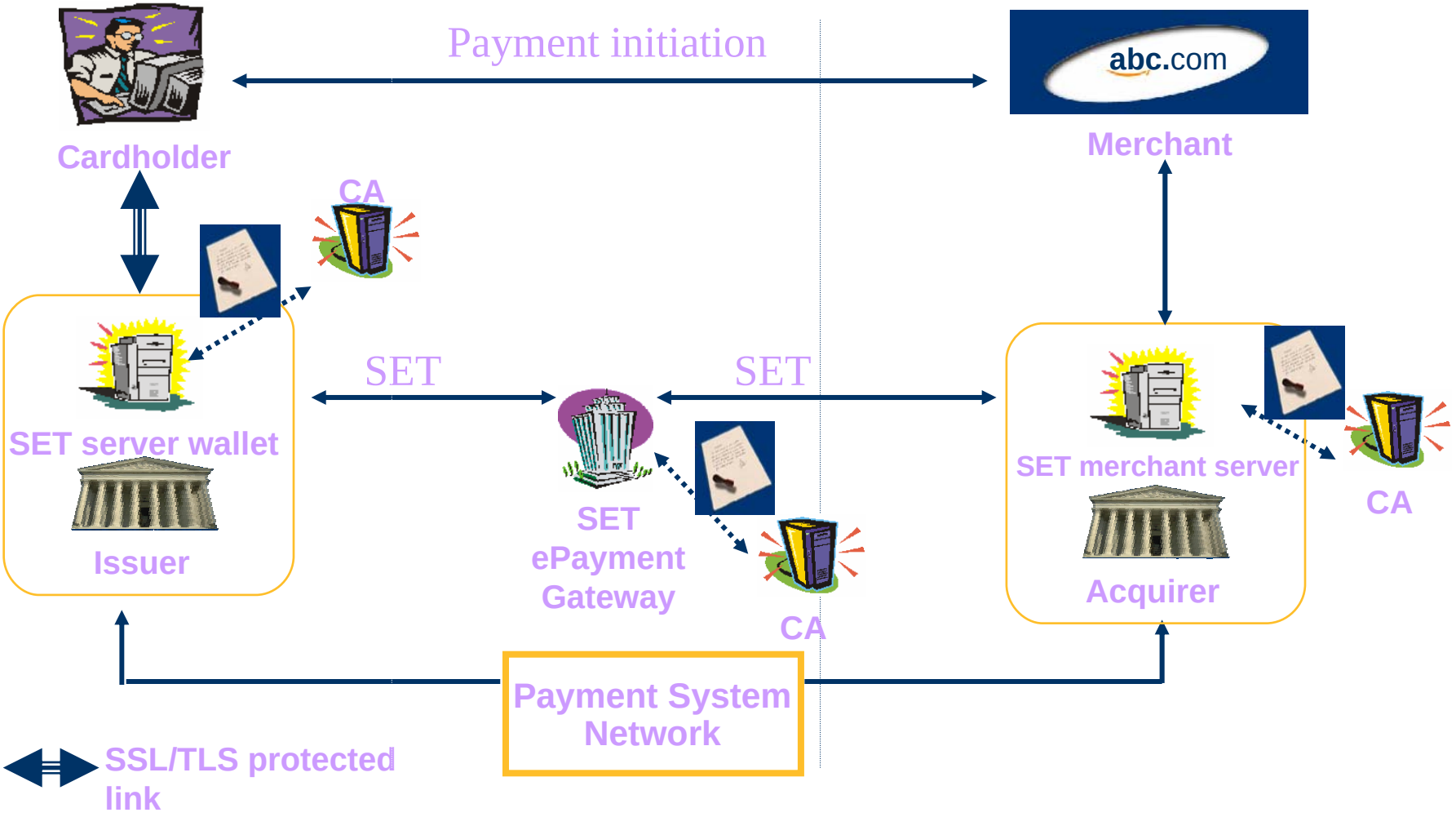
Secure Electronic Transaction (SET)



SET – analysis

- **Security considerations**
- Very secure: confidentiality and integrity, merchant and cardholder authentication, replay protection
- **Business considerations**
- Guarantee of payment for merchants, reduced charge-backs
- **Operational considerations**
- Distribution of certificates and portability
- Complexity of use and of implementation
- No device independence

3D-SET – description



3D-SET – analysis

- **Main changes to SET**
- Reliance on cardholder authentication online to the issuer (issuer-defined method)
- Certificates still used but held at server wallets
- Standardized payment messages required between issuer and acquirer domains

3-D SET improvements were not sufficient to drive significant financial institution investment – SET is now undergoing a decommissioning process within SETCo

3-D Secure – background

- Currently being deployed by both MasterCard and Visa.
- Was initially a Visa design but has now also been adopted by MasterCard.
- Supports cardholder authentication.
- Main incentive to merchant is liability transfer.

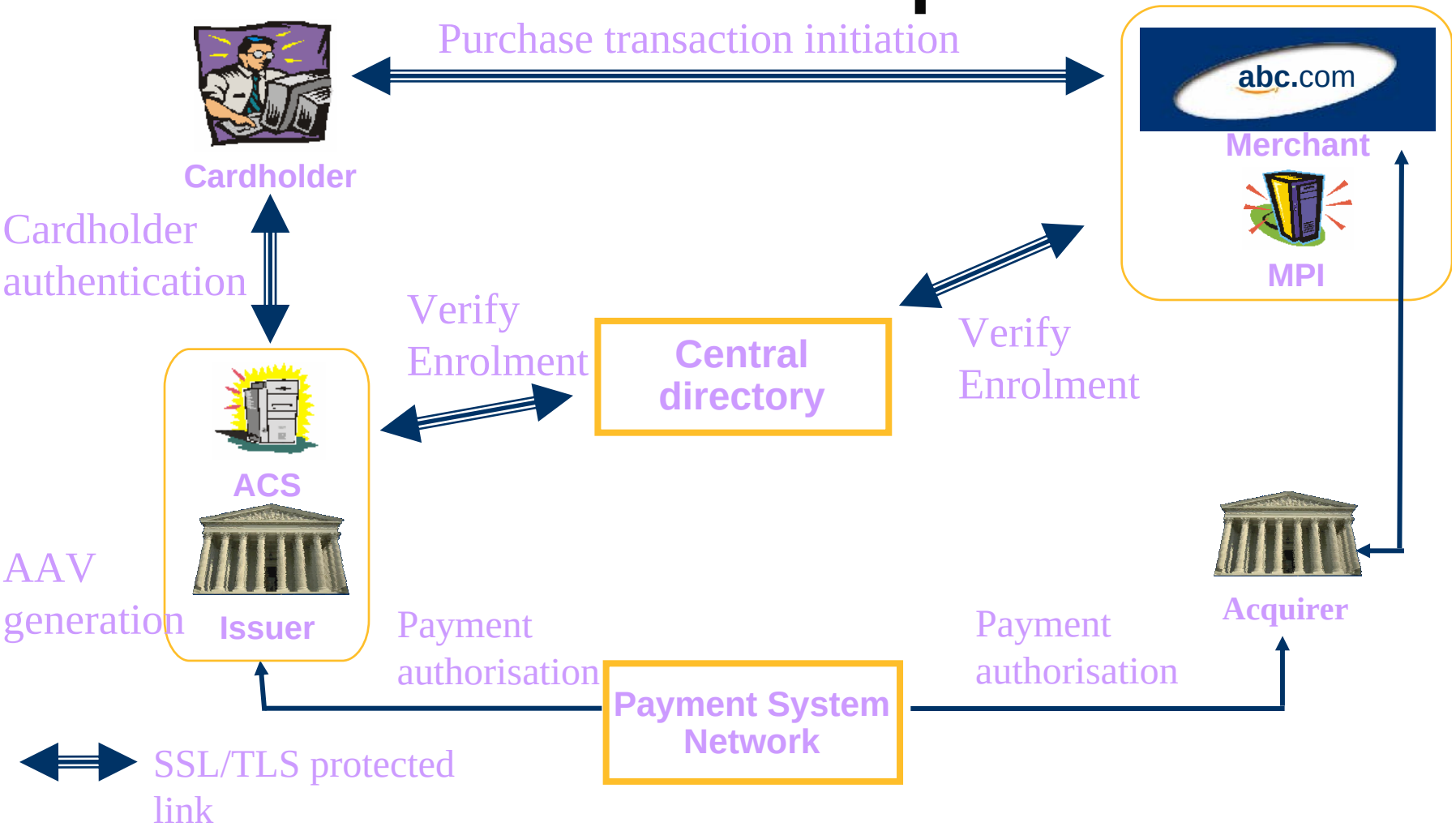
3-D Secure – technical approach

- Builds on existing ‘tried and trusted’ technology, including SSL/TLS.
- Minimises changes to current payment model.
- Based on negative experience with SET and 3D-SET.

3-D Secure – key players

- **Merchant:**
  - installs plug-in on server to talk to central 3-D Secure directory.
- **Issuer provides Access Control Server (ACS) to:**
  - authenticate cardholder;
  - generate and sign Account Authentication Value (AAV);
  - verify AAV as part of clearing process.
- **Cardholder:**
  - authenticates to issuer.
- **Acquirer:**
  - provides payment authorisation as at present (also verify AAV).
- **Brand:**
  - provides online directory server.

3-D Secure – relationships



3-D Secure – analysis

- **Security considerations**
  - Confidentiality and integrity linked to SSL security
  - Issuer-defined authentication method
  - Digital signature and Accountholder Authentication Value (AAV) as proof of cardholder authentication
- **Business considerations**
  - Guarantee of payment for merchants, reduced charge-backs
- **Operational considerations**
  - Ease of use: cardholders only need a browser to participate
  - Large number of messages sent to conduct a transaction

3-D Secure – cardholder authentication

- **Cardholder authentication mechanisms**
  - Chosen by Issuers
  - Prove knowledge or possession of authentication factor(s)
    - Something you know, something you have, something you are, something you do
  - Security evaluation
    - Number of factors involved, intrinsic security of factors, security properties of underlying mechanisms
- **Need for personal, pervasive factors**
  - Mobile devices, e.g. mobile phones may be a suitable solution

3-D Secure – cardholder authentication risks

- The scheme uses *http redirection* to redirect cardholder web browser from merchant server to Issuer ACS.
- This could be subverted to allow man-in-the-middle attack, where cardholder browser directed to ‘mock’ Issuer ACS.
- This could allow theft of cardholder password.
- Hence ‘static’ cardholder authentication not desirable.

3-D Secure – using EMV cards

- One way of allowing dynamic cardholder authentication at minimum issuer cost is to leverage EMV cards (existing secure token).
- MasterCard have deployed scheme where cardholders are issued with low cost personal card reader, and EMV card used to generate a one-time authenticator for Issuer ACS.

Future of Internet payment security

- 3-D Secure addresses some of security issues but not all.
- Merchant servers not protected, and there is no authentication of merchant to cardholder.
- Is this a long term problem?

3 Mobile Payments

Use of Mobile Devices

- **As authentication devices**
- Mobile (or rather SIM card) as authentication factor
- Mobile supporting an authentication mechanism
  - Mobile as PIN entry device
- **As access devices to support the whole payment phase**
- Mobile devices have scarce resources
  - This may preclude the implementation of some solutions
- The user interface is limited
  - Impractical user interfaces may create new threats and make data entry difficult

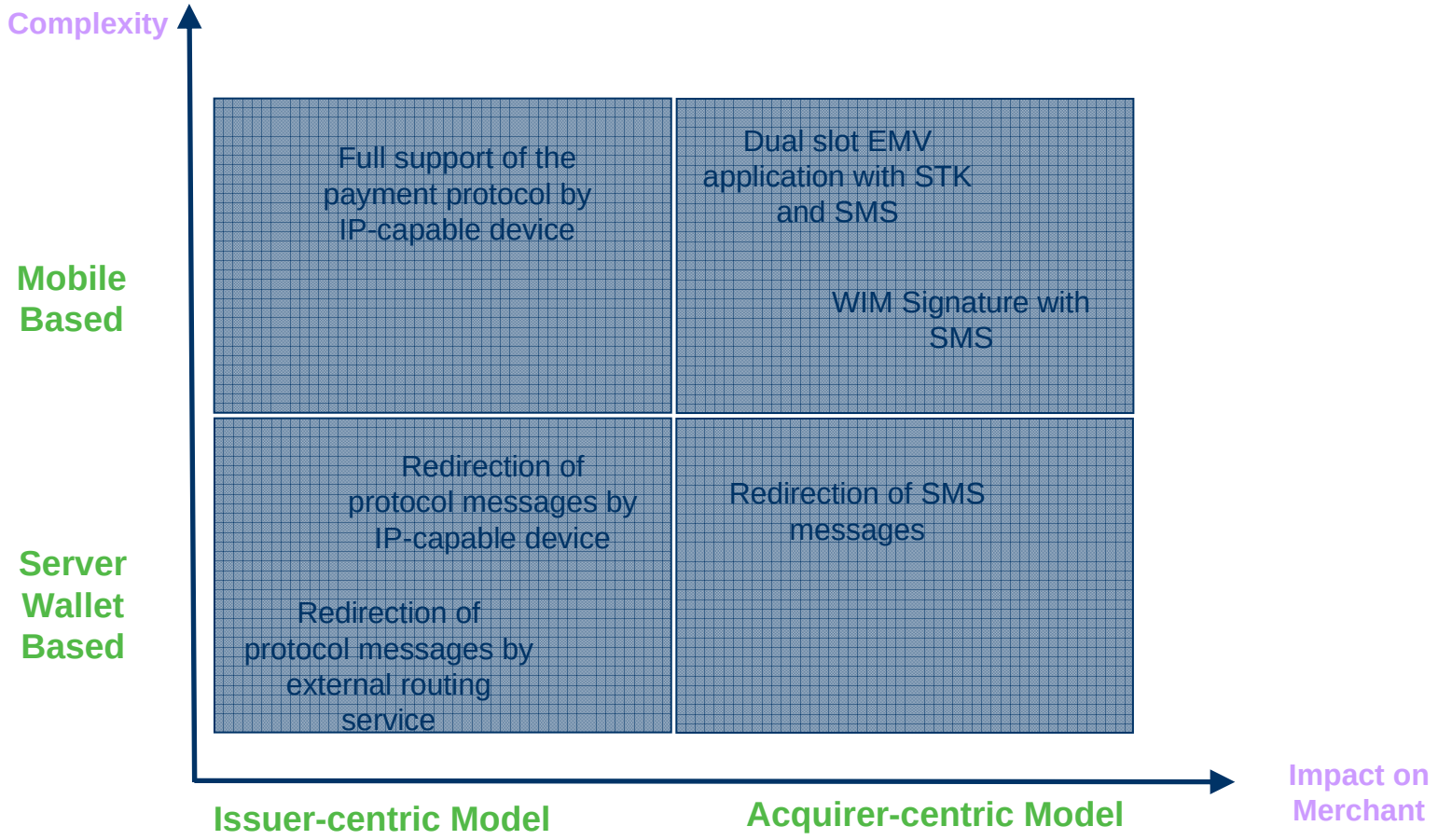
Characteristics

- **Personal nature**
  - Suitable for performing security functions (e.g. PIN entry) as less sensitive to tampering, keyboard sniffing, etc.
- **Pervasive nature**
  - May solve cost and distribution issues associated with massive rollout of tokens or specific hardware
- **Specific channels and protocols**
  - Particularities of channel (e.g. over-the-air link) and of protocols must be considered
  - Rapidly changing wireless standards

Two models

- **Acquirer-centric model**
  - Merchant in charge of handling the interactions with the mobile device
  - Usually relies on a mobile-specific protocol
  - Examples include dual chip and dual slot
- **Issuer-centric model**
  - Issuer in charge of handling the interactions with the mobile device
  - Merchant may be unaware of mobile nature of payment
  - Usually relies on a classical e-Payment protocol
  - Examples: mobile phone callback, WIM-based signature

Positioning of m-Payment Schemes



Current shortcomings

- **Authentication**
  - Reliance on personal nature of mobile device
  - Reliance on authentication by Telco, or need for additional mechanisms
- **Confidentiality and data integrity**
  - Reliance on the underlying mobile network security
  - No end-to-end security services
- **Non-repudiation**
  - Need for additional mechanisms, not widely deployed or not fully suitable

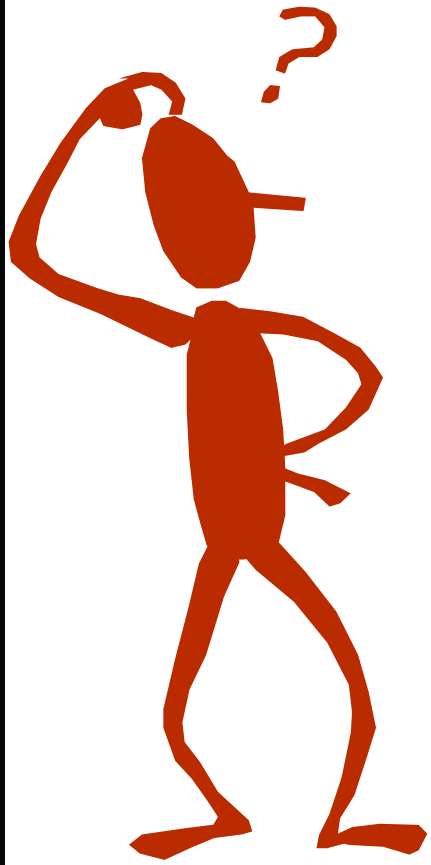
Mobile Payment Security Techniques I

- **2-way messaging**
  - PIN-based authentication
  - Define a common message flow using SMS messages
  - Define ‘Security Best Practices’
- **Proprietary systems**
  - Implementations rely on the use of SIM toolkit (STK)
  - STK applications may embed symmetric keys or have public key cryptographic functionalities
  - Requires co-operation with mobile operator(s)

Mobile Payment Security Techniques II

- **WAP**
  - Standardized and implemented on most phones
  - WAP offers security services (WTLS and application-level cryptographic library) but they rely on the use of a WIM
  - WIM stores key for WTLS authentication & key for signature of data
  - WIM functionalities often combined with SIM functions

Contact



Chris Mitchell

Information Security Group
Royal Holloway
University of London

www.isg.rhul.ac.uk/~cjm
C.Mitchell@rhul.ac.uk