Electronic money, electronic identity impact on telecommunications

Smart Card based solutions

Lauri Pesonen
SETEC OY

TELECOM FORUM 1998
Wednesday, 4 November

Contents of the presentation

- electronic identity in open networks
  - electronic transactions in open networks
  - basis of cryptography
  - public key smart cards
  - public key infrastructure
  - services and schemes
- electronic money in open networks

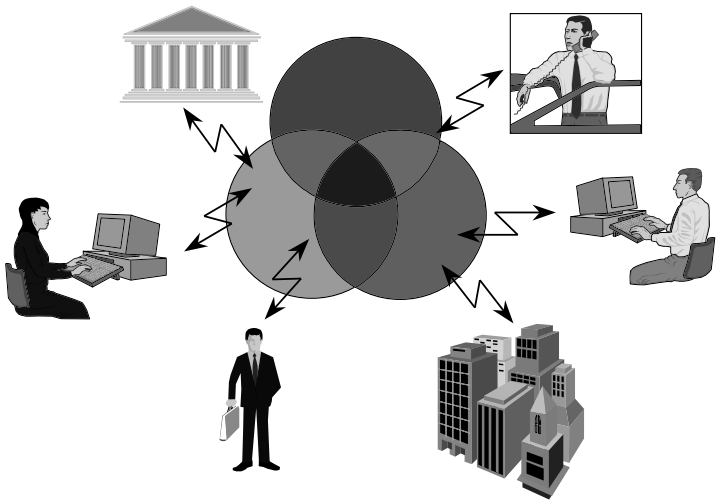
1. Electronic identity in open networks

Electronic transactions

- electronic transactions in open networks are rapidly increasing
- private sector is adopting (part of) its business into open networks
- the administration and public service is also becoming increasingly active
- basis of any transaction, including electronic, is a realible and secure authentication of the communicating parties
- electronic transactions in open networks are an important and essential part of the information society

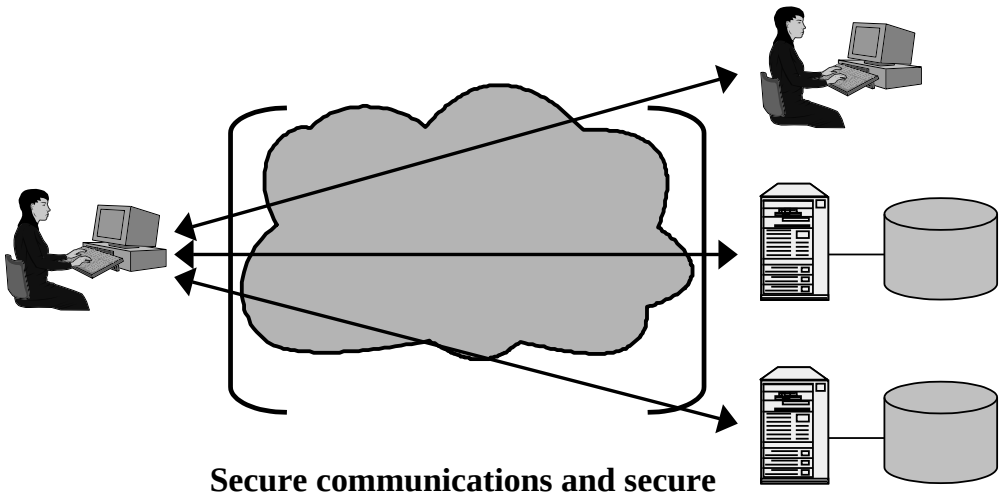
SETECOY

Electronic transactions in open networks



SETECOY

Secure transactions in open networks

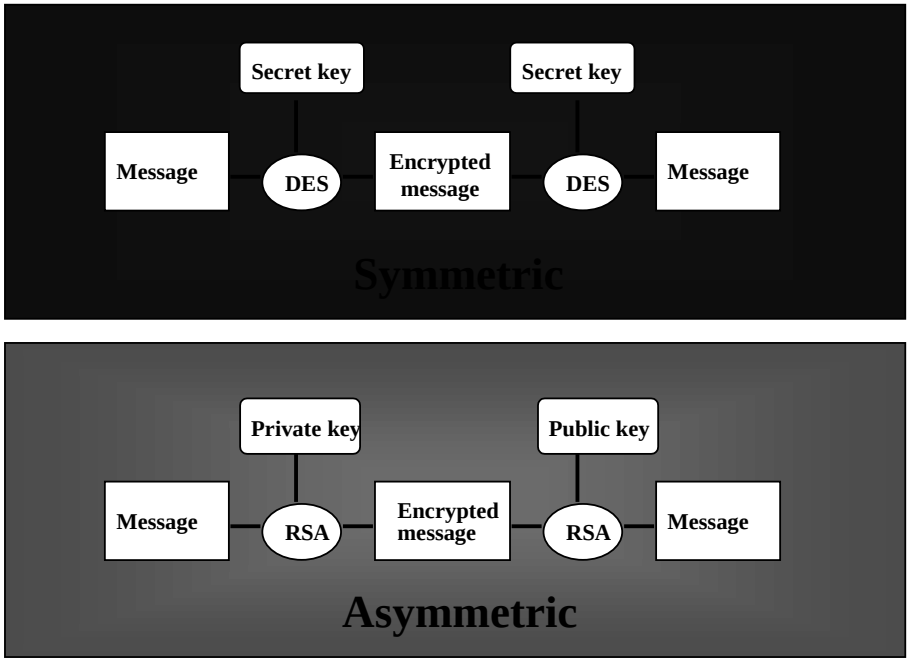


Secure communications and secure transaction between users and IT systems

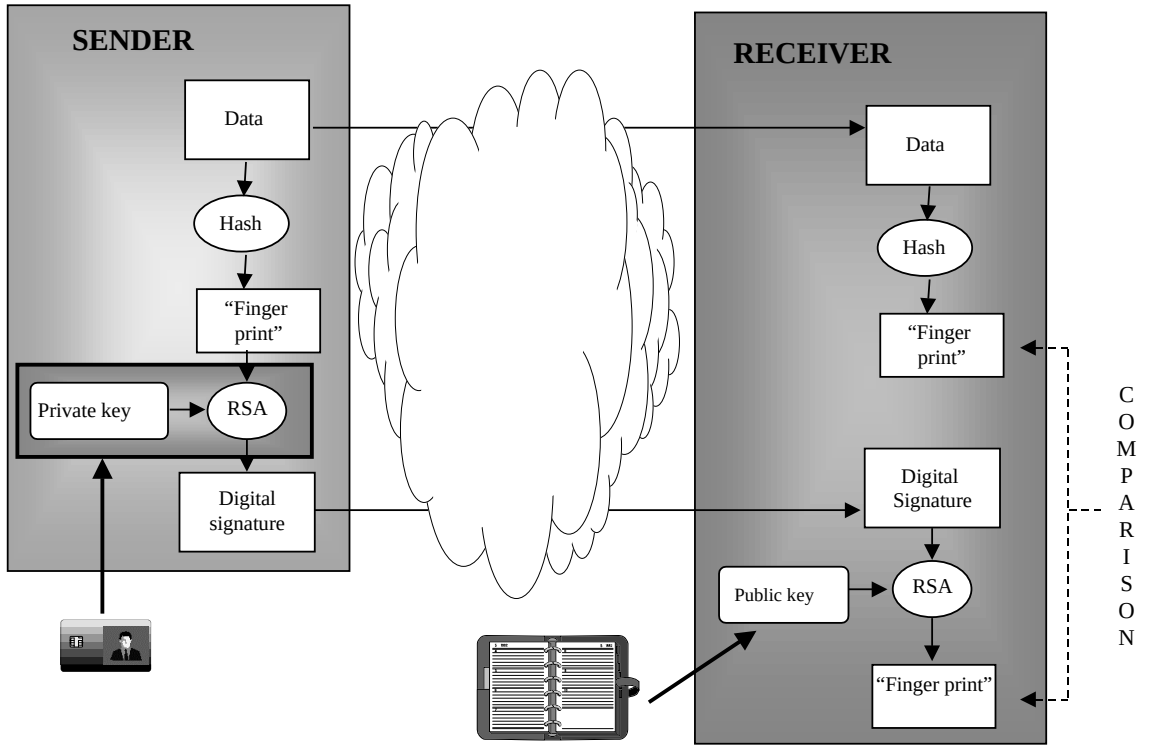
Information security requirements in open networks

- strong authentication of communicating parties (i.e. identification)
- digital signatures for
  - proof of origin
  - integrity of information
- confidentiality of information
- non-repudiation of transaction

Basics of encryption algorithms



Digital signature

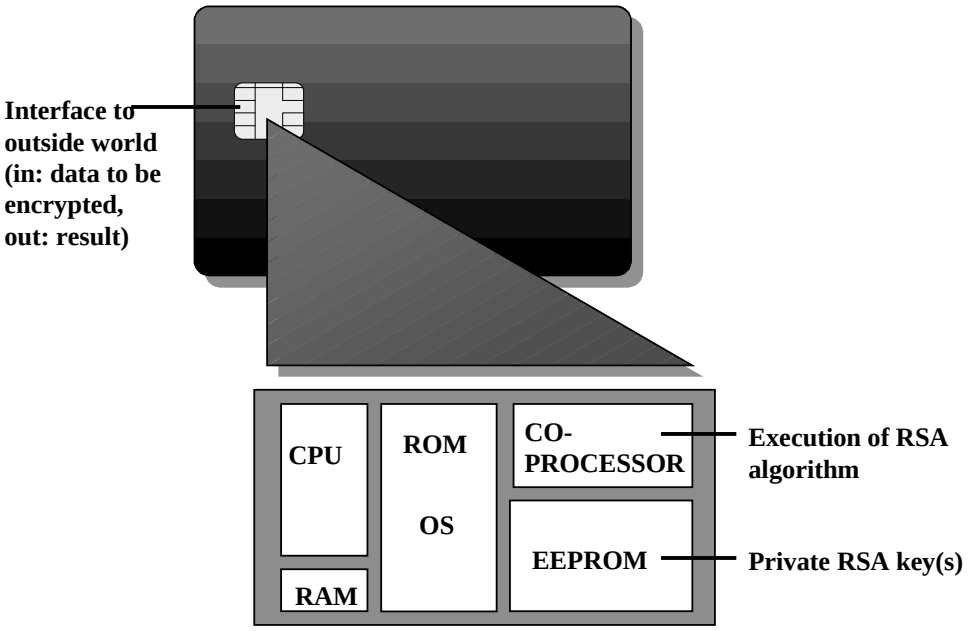


Implementation of security services

- each user (or process) has one or more RSA key pairs
- private RSA key is to be available only for the owner of the key (i.e. user) while public RSA key shall be available to all users
- private RSA key is used for the following services
  - digital signature, integrity of information, non-repudiation of the transaction
  - strong authentication
- public RSA key (of the recipient) can be used to provide confidentiality of information

-> PKI = PUBLIC KEY INFRASTRUCTURE

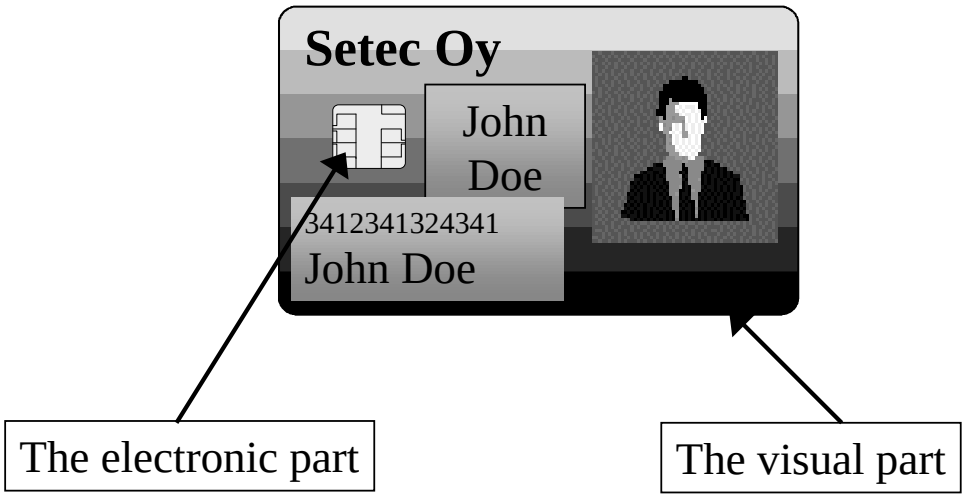
Smart card and public key algorithm



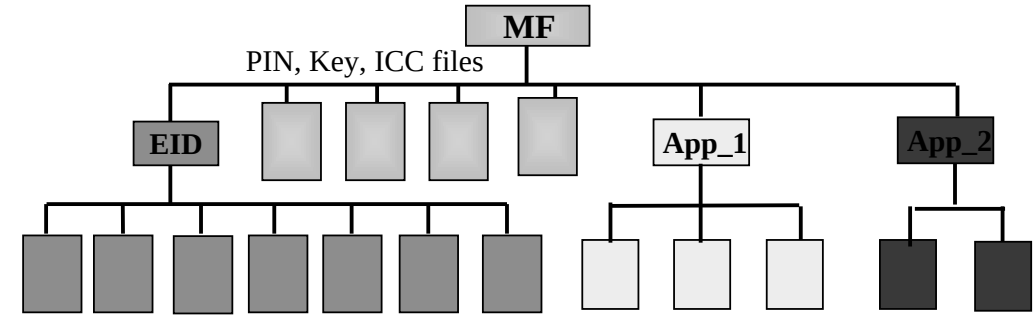
The advantages of smart card

- private RSA key(s) are processed only inside the card -> keys cannot be compromised or copied
- PIN authentication used for card holder authentication -> only authorised person can use the private RSA key(s)
- smart card is portable -> the secure public key services are available everywhere in the infrastructure
- can be combined with other security sensitive chip applications
- can be combined with the official visual ID card

Electronic ID card

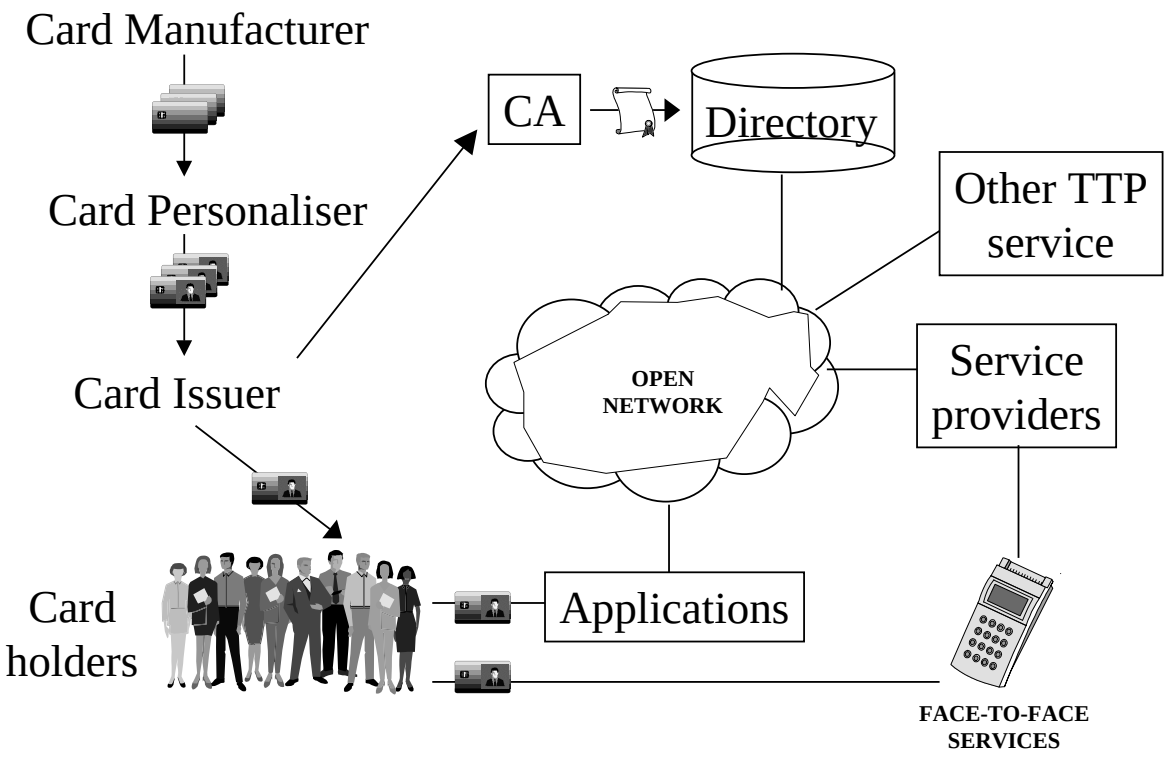


Example of multiapplication ELID card data contents



Electronic ID application containing
- private RSA key for digital signatures
- private RSA key for authentication and encryption
- public key certificate (signatures)
- public key certificate (authentication and encryption)
- CA's public key (as a certificate)
- configuration information (for example key usage)

Public Key infrastructure



Certification Authority (CA)

- Certification Authority (CA) is an essential trusted third party (TTP) in the public key infrastructure; CA has its own RSA key pair(s)
- CA is responsible for
  - certifying the authenticity of the user's public RSA key -> public key certificate
  - maintenance of certificate revocation lists (CRL)
  - distribution of CA's own public key
- infrastructure may include more than one CA
- infrastructure contains a so called root-CA, who is trusted by everybody and whose public key is not presented in a certificate format

Directory service

- directory service is used in the public key infrastructure for
  - distribution of certificates
  - distribution of CRLs
- directory service shall
  - be available for all users, applications, services
  - enable the communication between different directory (servers)
- infrastructure may include more than one directory service
- directory can be used, of course, for distribution of other information too

Other trusted third party services

- Time stamp service
- Notary

SETECOY

Examples of services and applications

- services by public authorities
  - access to registers
  - electronic forms and applications
- internal use in public administration
- electronic commerce
- business-to-business communications
- private sector
  - banking services, insuarance services etc.
- protected communications (for example email)
- logical access control (for example remote work)

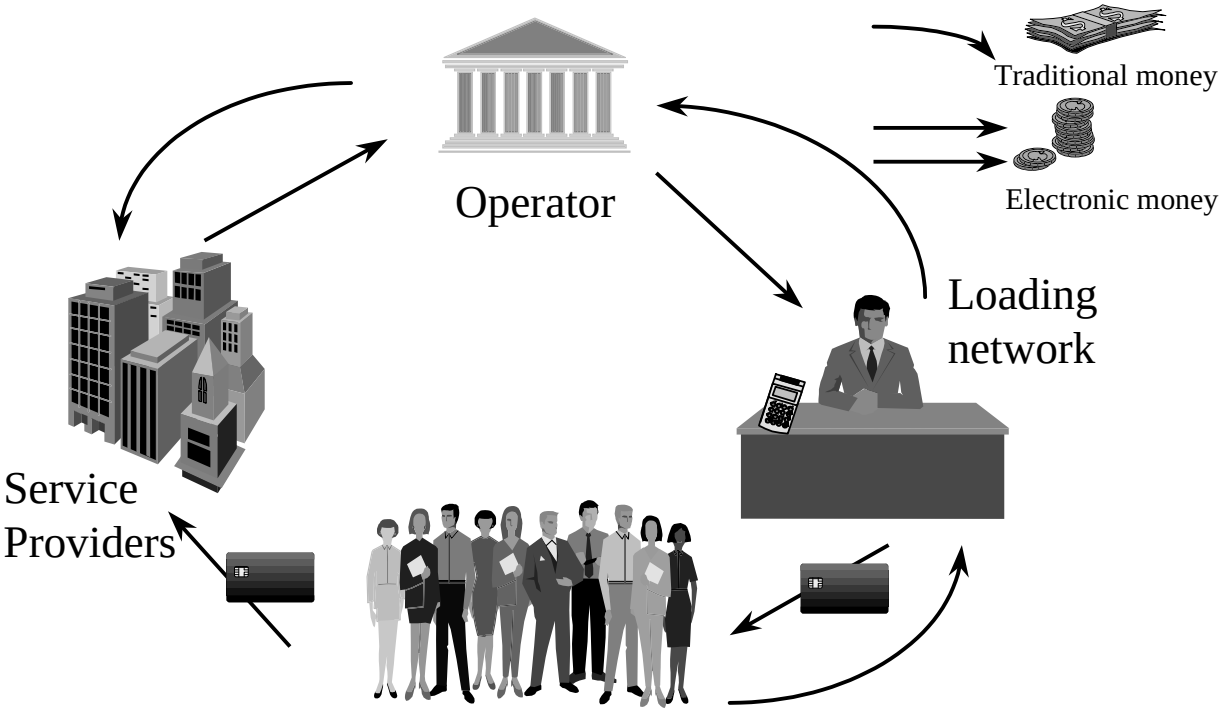
SETECOY

National electronic ID card schemes

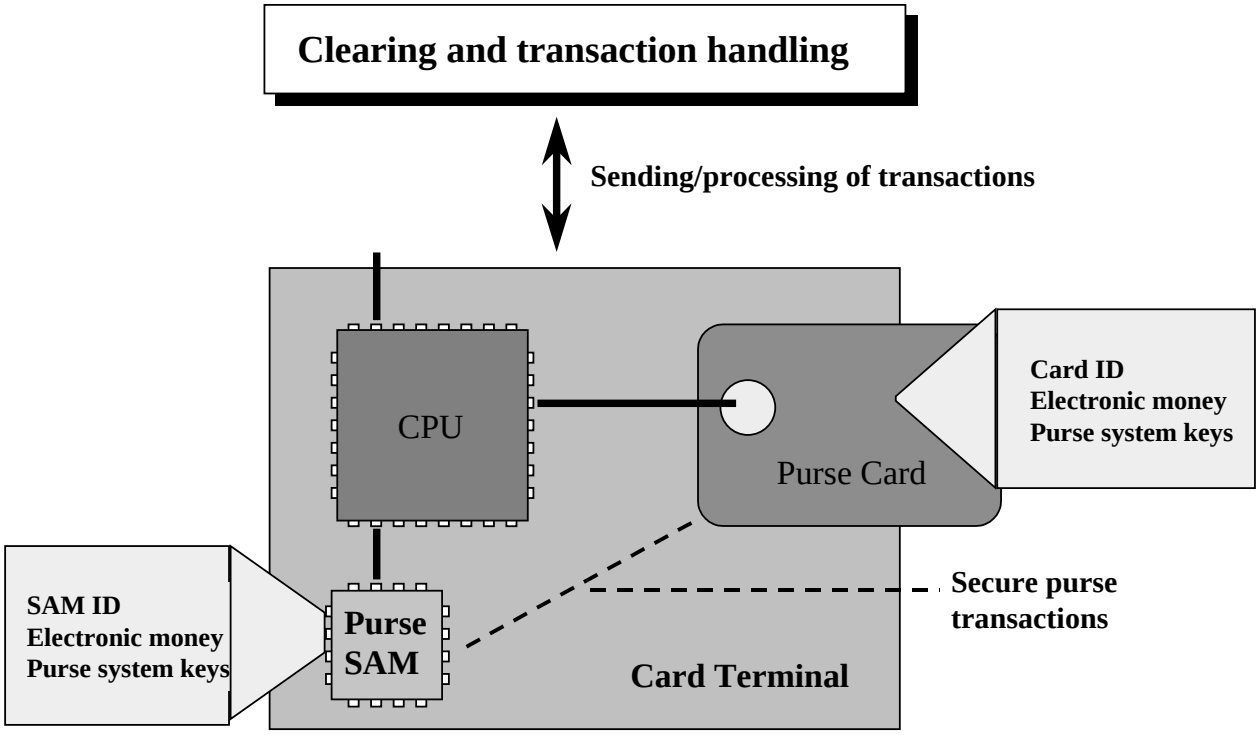
- Sweden: national electronic ID card in use (SEIS)
- Finland
  - HST: national electronic ID card - pilot phase
  - NovaSec: initiative for private sector - pilot phase
- Germany (digital signature law -> requires ITSEC E4 level evaluation)
- Italy (digital signature law)
- Malaysia: Government Multipurpose Card
- Taiwan: national electronic ID card
- Singapore: national electronic ID card RFP coming out

2. Electronic money in open networks

Electronic Purse system

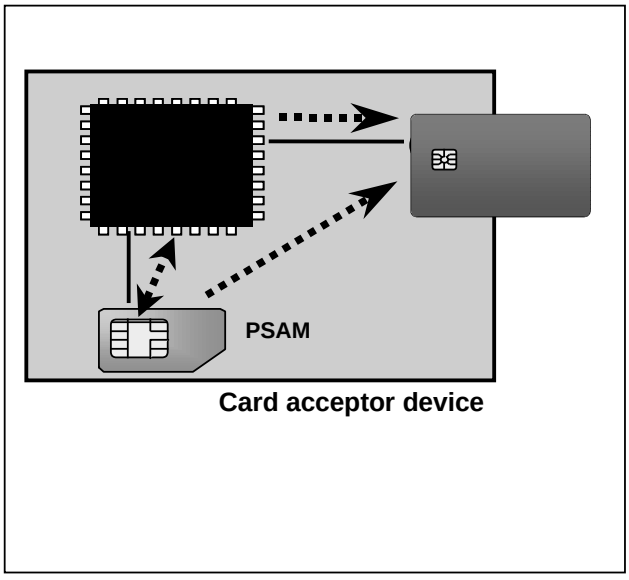


Key components of electronic purse

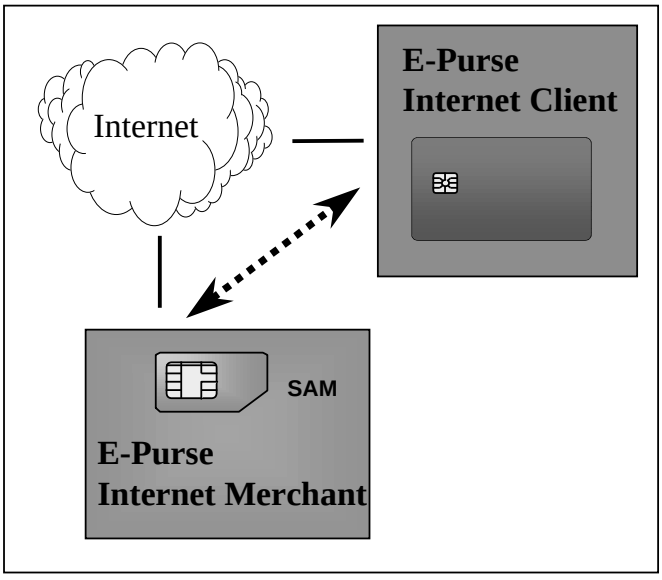


From terminal to internet purchases

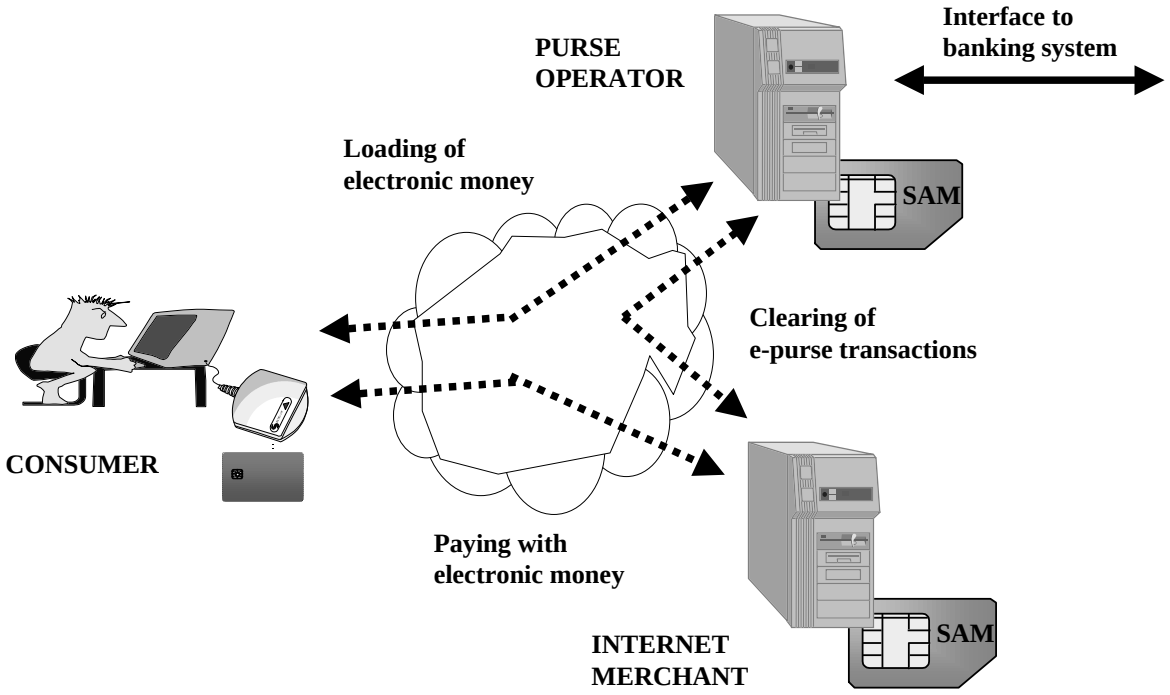
Terminal purchases



Internet purchases



Internet payment concept overview



About e-purse payments in internet

- requirements
  - secure
  - cost-effective
  - anonymous (possible requirement)
- typically small payments
- examples of purchased items
  - information
  - viewing time
  - reservations, tickets etc.

CONCLUSION

Business transactions in open networks