P-A Pays & P. van der Linden
GC Tech
July 1995

GC Tech Transaction Model

Clearing in the Middle Transaction Model

overview

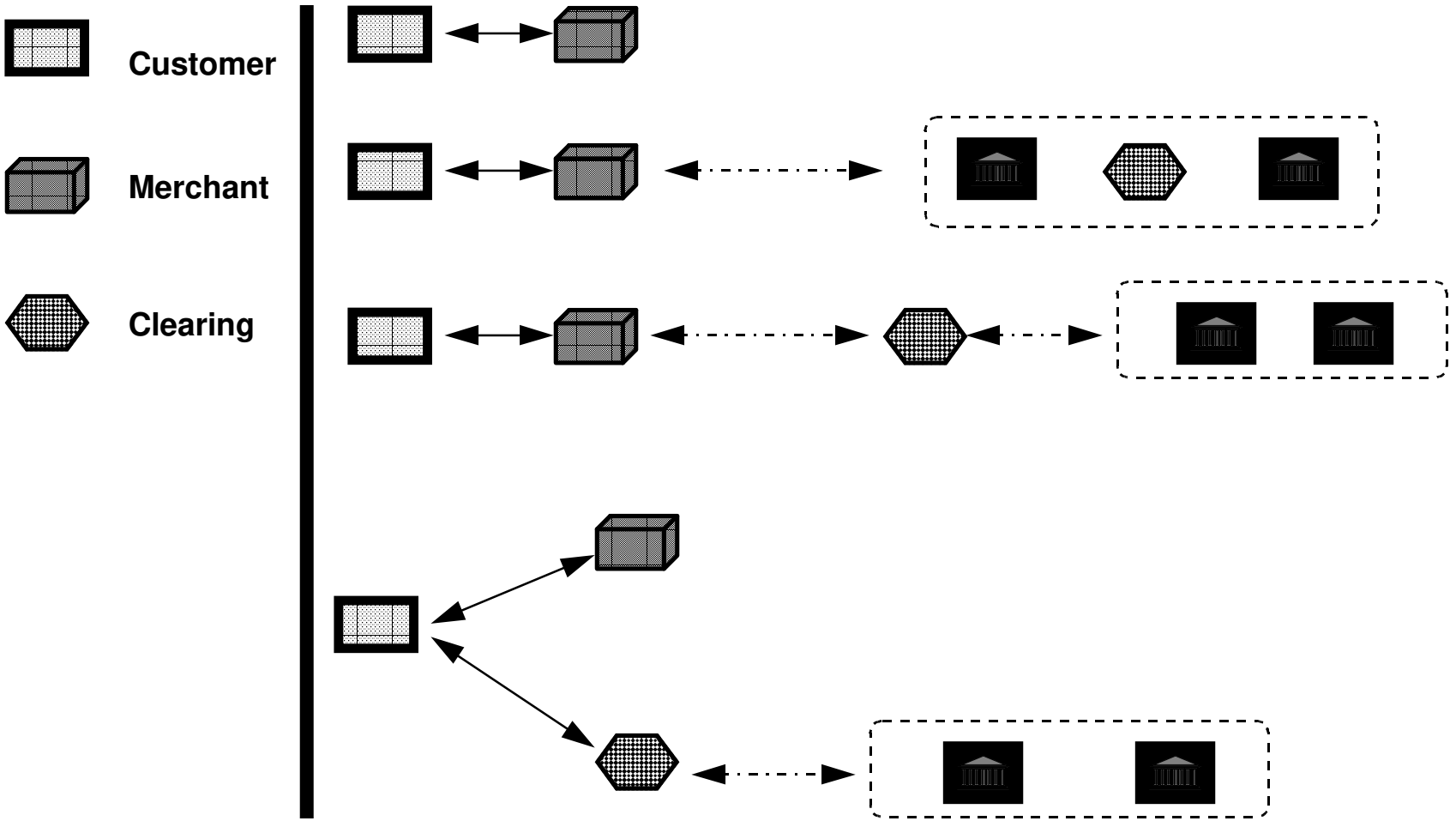
Paul-André Pays & Pieter van der Linden

33rd IETF

E-Payments Transaction Models

P-A Pays & P. van der Linden
GC Tech
July 1995

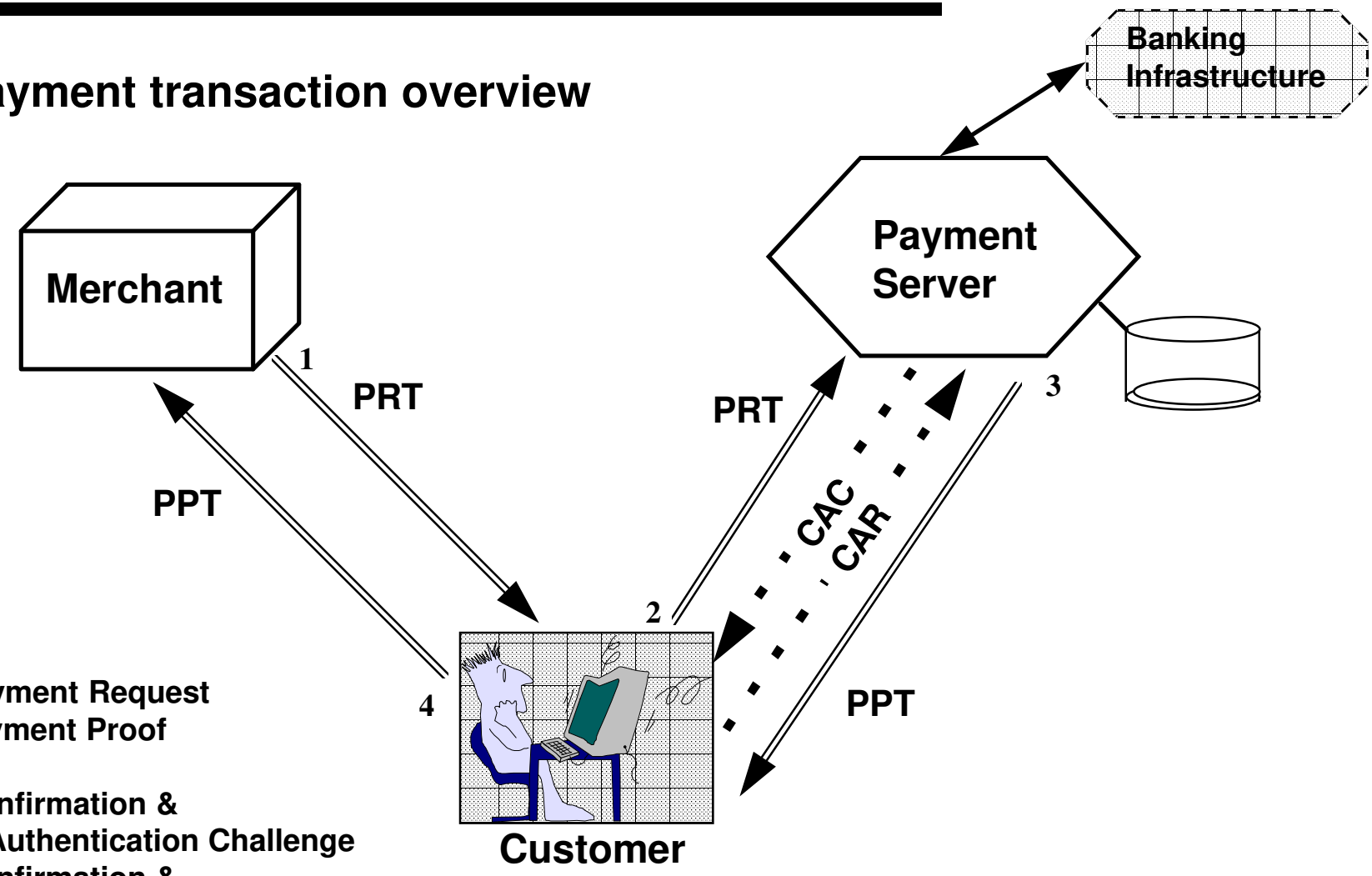
- **just a reminder**



CMTM : Clearing in the Middle Transaction Model

P-A Pays & P. van der Linden
GC Tech
July 1995

- **Payment transaction overview**



PRT : Payment Request
PPT : Payment Proof

CAC : Confirmation & Authentication Challenge
CAR : Confirmation & Authentication Response

CMTM features (1)

P-A Pays & P. van der Linden
GC Tech
July 1995

- **Maximal transaction security : Payment server**
  - **provides customers AND merchants guarantees**
  - **provides customers AND merchants additional services**
    - **management of *electronic wallets***
      - **for macro and micro payments**
    - **payments proofs and *duplicata***
  - **is the *only* entity to be trusted**
- **Minimal cyphering requirements**
  - **no secure channel required between C and M**
  - **cyphering use limited to *authentication* and *integrity***
  - **acceptable by any (known) cyphering laws**
- **Networked transaction efficiency**
  - **minimal number of low level exchanges**
  - **thanks to CPTP**
    - **(Customer Payment-server Transaction Protocol)**

CMTM features (2)

P-A Pays & P. van der Linden
GC Tech
July 1995

- **A limited level of anonimity**
  - **using it's own namespace (not Visa or Bank ones)**
  - **CustomerID : indicates 1) Currency, 2) Payment-Server**
- **M (Merchant server)**
  - **absolutely independant (from any P or any other M)**
  - **provided with a Merchant Tool-Kit & a certificate**
- **PRT (Payment Request Ticket)**
  - **requ : authentication, integrity**
  - **sol : signed by M**
- **PPT (Payment Proof Ticket)**
  - **requ : authentication, integrity**
  - **sol : signed by P**
- **CAC & CAR**
  - **req : authentication, non repudiation, NO replay**
  - **sol : challenge response for an explicit confirmation and authentication**

C <-> P communication

P-A Pays & P. van der Linden
GC Tech
July 1995

- only secure channel required
- 2 differents layers
  - EPAP : Electronic Payment Application Protocol
    - for user-level operations such as
      - payment
      - electronic wallet status
      - electronic wallet refill
  - CPTP : Consumer Payment-server Transaction Protocol
    - see next slide

CPTP : Customer Payment-server Transaction Protocol (1)

P-A Pays & P. van der Linden
GC Tech
July 1995

- **used between C and P**
  - **to provide the required security**
  - **to carry EPAP (E-payment level) operations**
- **C (the customer)**
  - **is provided with a EPAP/CPTP capable client software**
  - **is registered with a CustomerID and a secret by P**
  - **knows P public key**
- **P (the payment server)**
  - **is provided with an asymetric key pair**
  - **maintains a customer authentication data-base**
  - **maintains an Electronic Wallet for each customer**
  - **maintains an Electronic Cash Register for each merchant**
  - **implements EPAP services (upon customer request)**

CPTP : Customer Payment-server Transaction Protocol (2)

P-A Pays & P. van der Linden
GC Tech
July 1995

- **(1) C -> P : Request**
  {Operation, Parameters, AddInfo } ***not signed***
- **(2) P -> C : Conf. & Auth. Challenge**
  {SeqNum, TimeStamp, CustID, AddInfo } ***signed by P***
- **(3) C -> P : Response**
  { CKrand, H(CustSecret) } ***encrypted with P public key***
  { SeqNum, TimeStamp, CustID, Info } ***signed with CKrand (using a MAC)***
- **(4) P -> C : Result**
  { result } ***signed with CKrand***
- **(4') P -> C : Error**
  { error } ***signed by P***

CMTM highlights

P-A Pays & P. van der Linden
GC Tech
July 1995

- use of traditional financial model
- minimal cyphering requirements
  - laws and regulations
  - efficiency
- minimal client site constraints
- maximal merchant autonomy
- multiple currencies
- transparent micro and macro payments
- competition between payment servers
  - value added services (rates, additional services, aso)
- open to authentication technology evolution
  - emergence of CA infrastructure(s)
  - hardware authentication devices

Adopted by Globe Online