Electronic checks and account transfers

Chapter 5.2

Agenda

5.1 Payment transfer between centralized accounts

5.2 FSTC payment initiatives

5.3 NACHA Internet payments

5.4 NetBill

5.5 NetCheque

5.6 Summary

FSTC payment initiatives

- Financial Services Technology Consortium
- A group of U.S. banks, research agencies, and government organizations

FSTC Projects

- Electronic checks
  - Bank infrastructure for e-commerce
- Investigate how existing bank payment systems, (e.g ACH payments) could be securely initiated over the Internet.
- How banks could act as trust brokers on behalf of their customers,
- Moving ATM to the Internet (future project)

Electronic check concept

- The check is in electronic form
- New services
  - Immediately verify funds availability
  - Security (digital signature validation)
  - Integrate into electronic ordering and billing processes

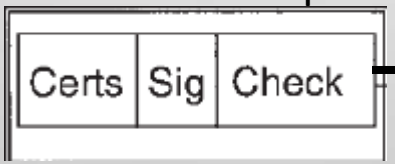
FSTC Electronic Check

Payer

Invoice

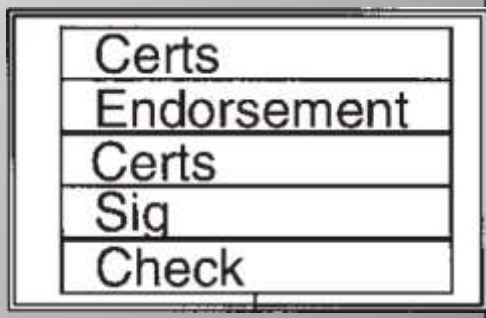
Payee

Secure Envelops



Electronic Check

Secure Envelops



E-mail
Statement

Payer's bank

Debit Account

ACH check clearing

Payee's bank

Credit Account

Other Checks

- Traveler's check
  - Changing the currency
- Certified check
  - Applying a bank's digital signature

Electronic Checkbook Device

- Electronic checkbook device
  - secure hardware
  - securely store secret-key and certificate information
  - Maintaining a register of what checks have been signed

Financial Services Markup Language (FSML)

- To define the structure and contents of an e-check
- FSML is specified using the (SGML)
  - A block to represent the contents of a check
  - Account block
  - Invoice block
  - Endorsement block
  - Signature block
  - Cert block
- FSML allows individual blocks to be signed,

Example FSML electronic check

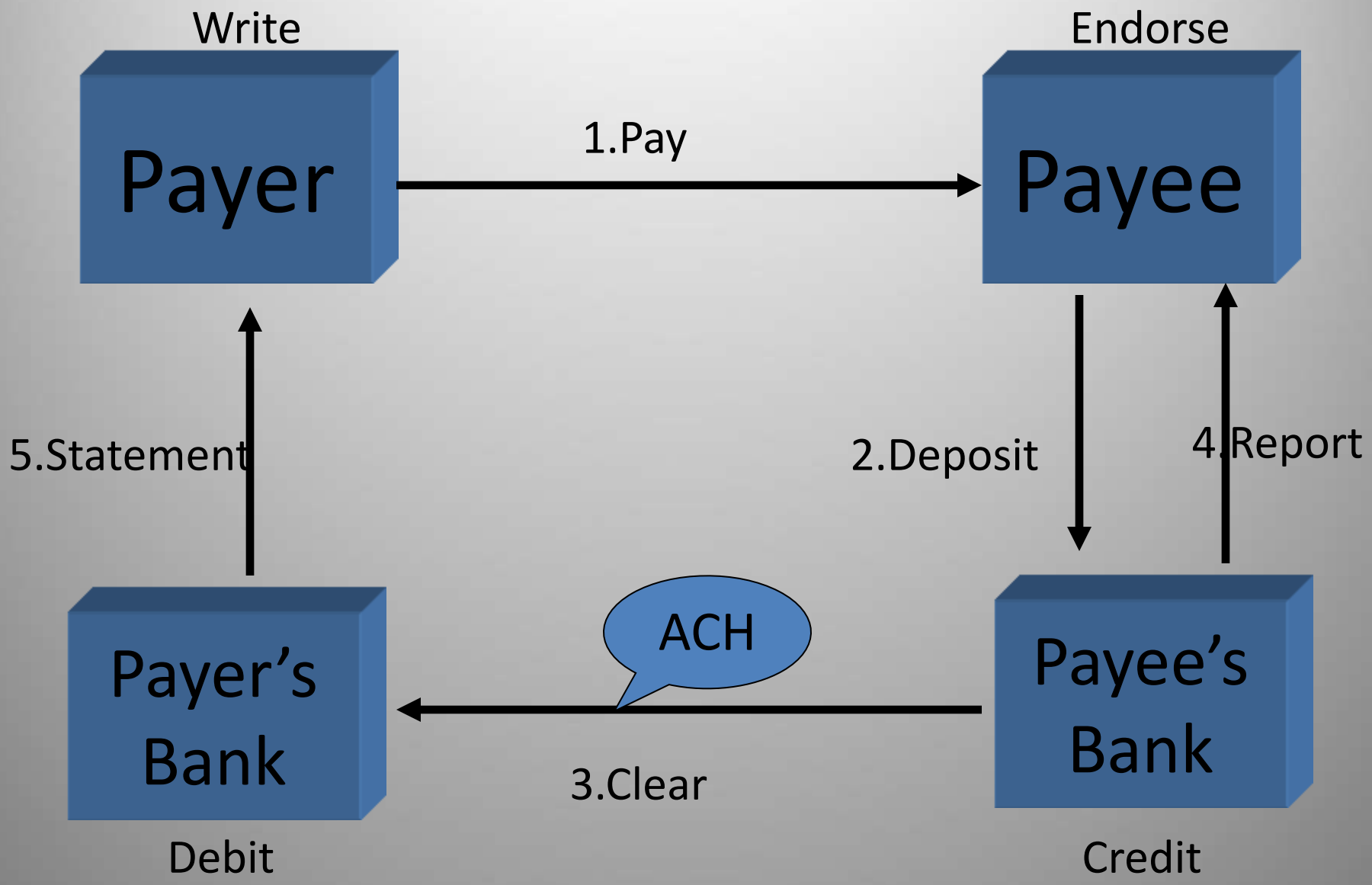
```
<fsml-doc docname="echeck204" type="check">
<check> <blkname>check1 <vers>1.0
<checkdata> <checknum>187 <dateissued>20010719 <datevalid>20010719
<country>us <amount>250.00 <currency>usd <payto>John E. Smith
</checkdata>
<checkbook>2048 <legalnotice>This instrument subject to check law
</check>

<signature>
<blkname>sig7 <vers>1.5
<sigdata>
<blockref>check1 <hash alg="sha">vFnS/1Vm9QaRDFAgtijkE24cazk=
<blockref>acct-11111111-00000001
<hash alg="sha">fF51C8MwtSVgeCQP0mzDTBjy1Zg= <nonce>9D9BC5AA75
<sigref>acct-11111111-00000001 <sigtype>check
<algorithm>sha/rsa <location>us </sigdata>
<sig>
Jinh43b1zYIydAELCmAo6j8nY/I=:KquV+Pas9mFrnDoD3wtQKVoWIpU56JK3WioPaNjXJ
7XcMnoISvEI3XB7WICVBN4TI2viUoWXB0XD1GJ3rXvb2XM3rC9EVX6MLNXCp2sxXVva23=
</signature>
```

Electronic check functional flows

- payment scenarios
  - deposit-and-clear
  - cash-and-transfer
  - lockbox
  - funds transfer

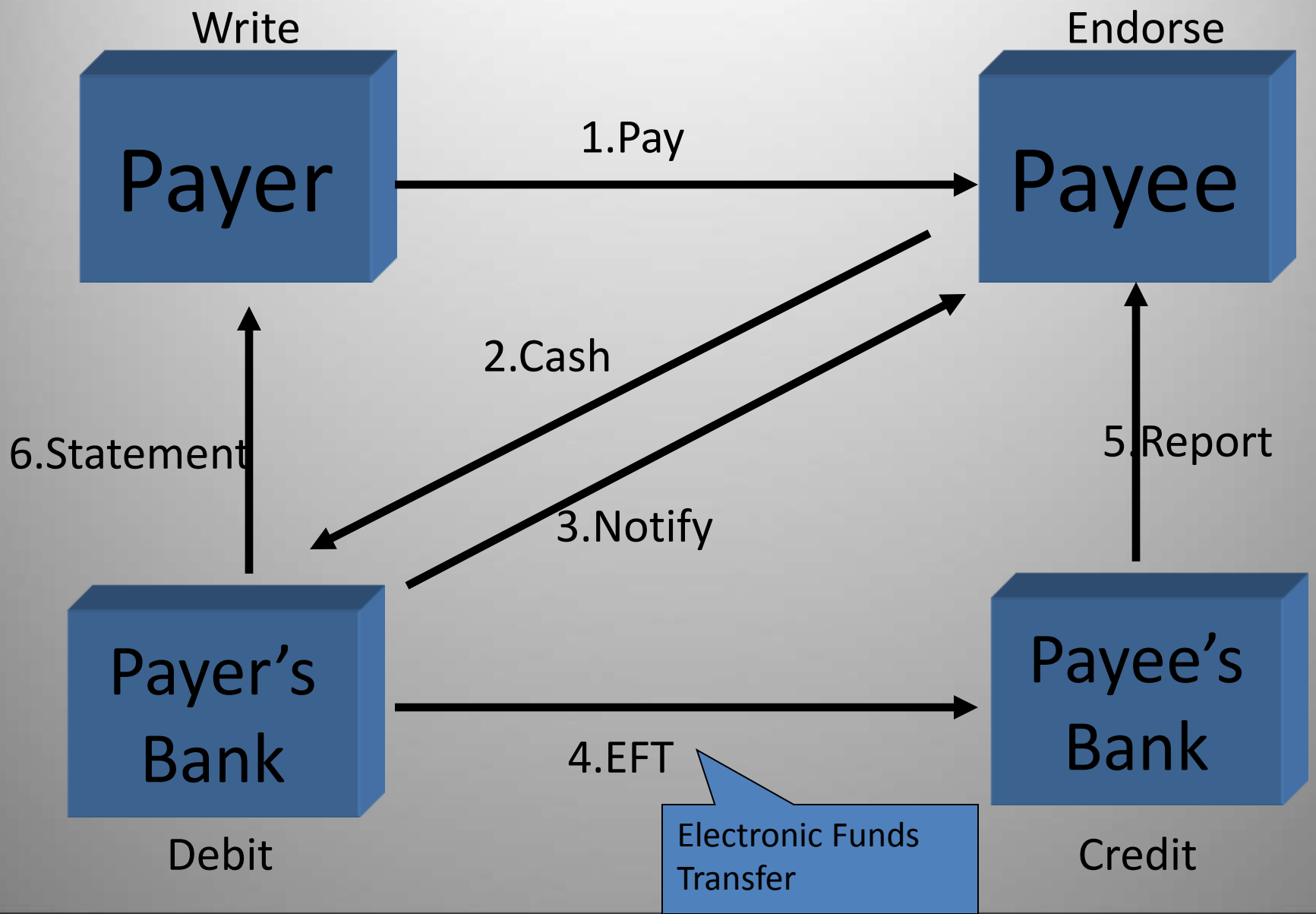
deposit-and-clear



deposit-and-clear

- Disadvantages
  - All parties must have their networking and processing capabilities upgraded to deal with electronic checks, before a single payment can be made.

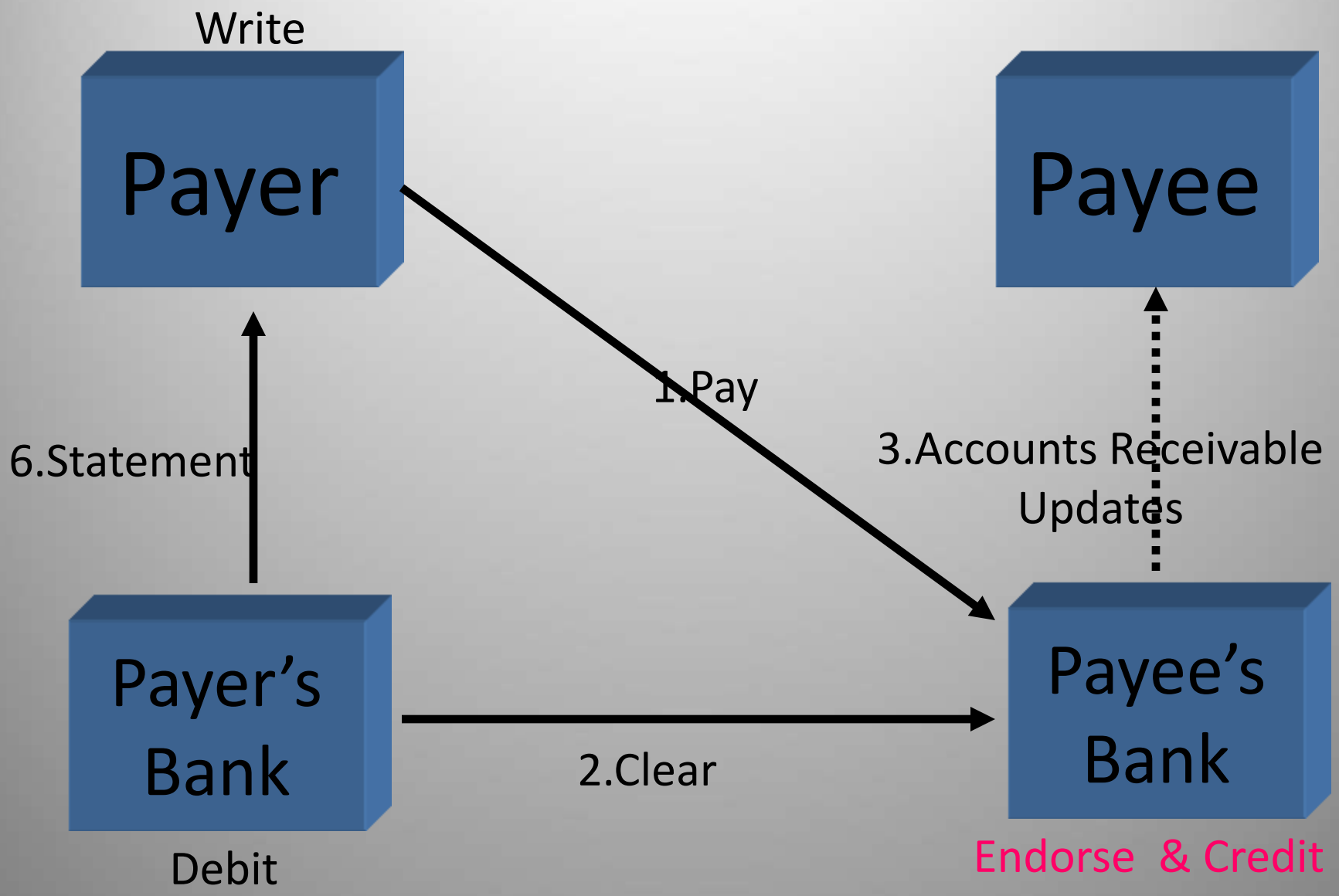
cash-and-transfer



cash-and-transfer

- While the payee can accept checks electronically, his bank cannot.

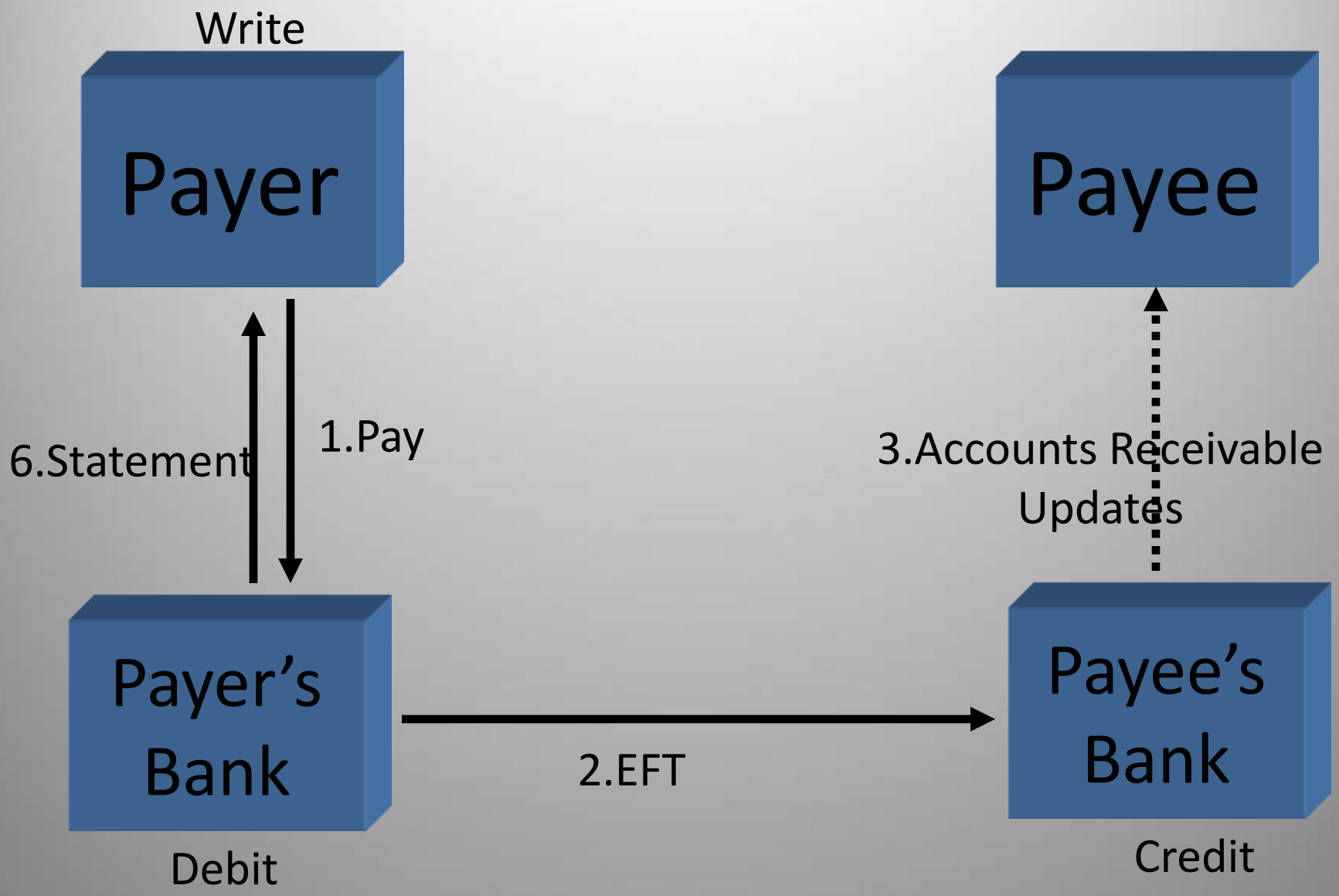
lockbox


Write
Payer
Payee
1.Pay
6.Statement
3.Accounts Receivable
Updates
Payer's
Bank
Payee's
Bank
2.Clear
Debit
Endorse & Credit

lockbox

- The electronic check is sent not to the payee, but to the payee’s bank.

funds transfer



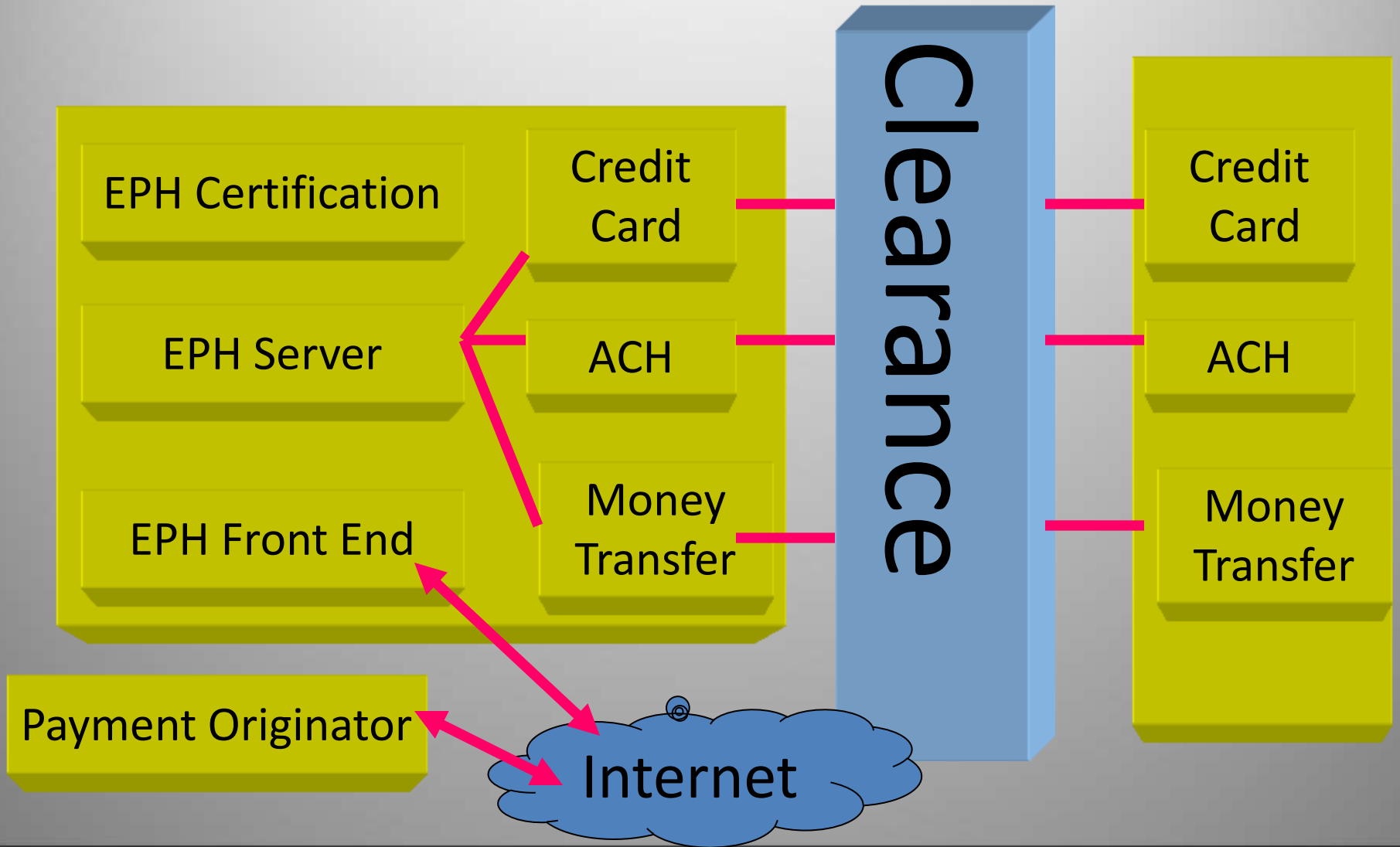
funds transfer

- In this case, only the payer's bank needs to be equipped to process electronic checks, as all other flows are handled by existing bank messaging systems.

Check-handling infrastructure

- Electronic payments handler (EPH)
  - Interface to the Internet and communicate
  - EPH server,
  - Certification server

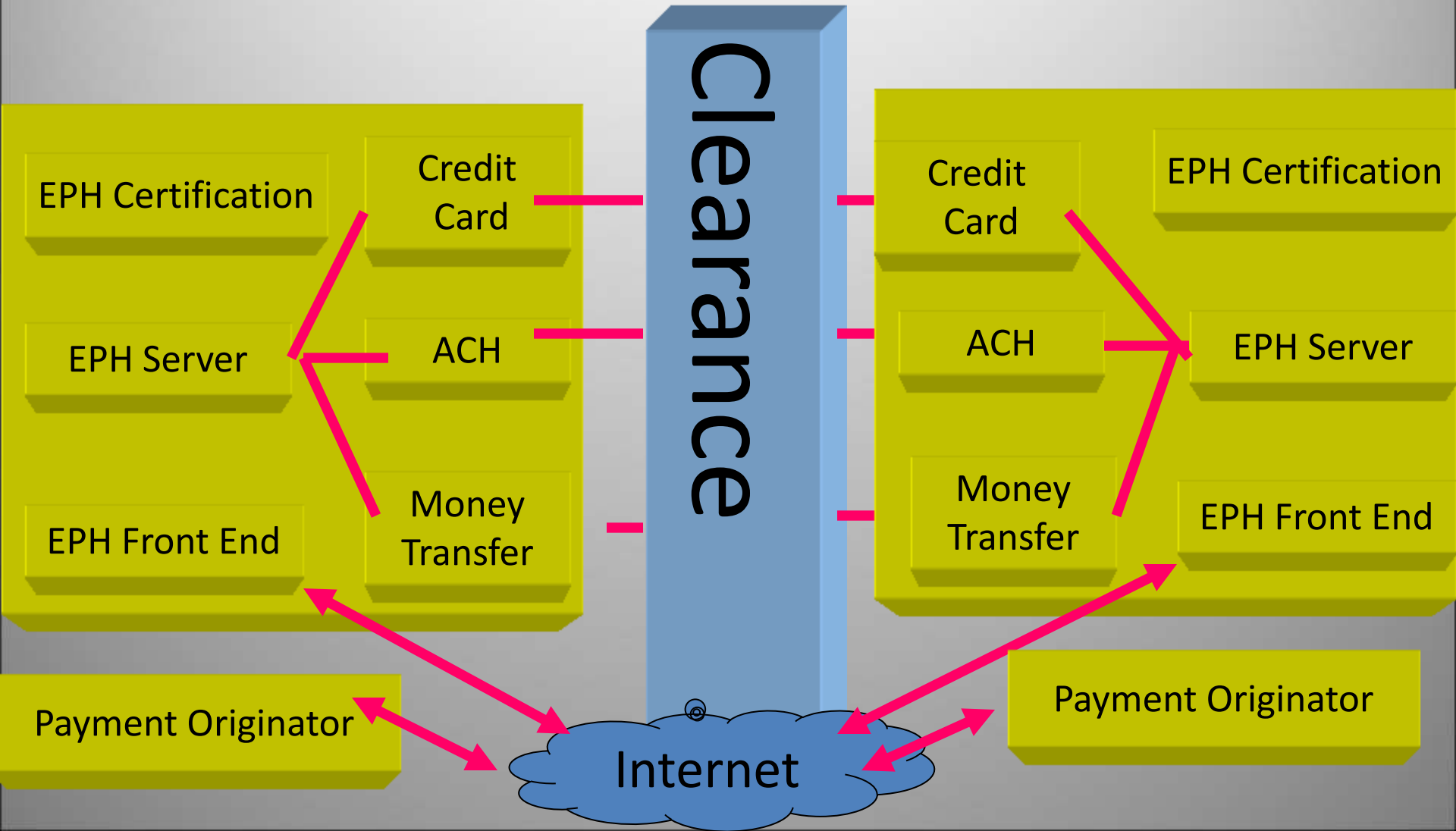
The interaction between the electronic payments handler (EPH) and existing payment systems



Phases of the deployment of the electronic commerce infrastructure

- phase 1
  - Only the originator's bank is equipped with EPH subsystems
- phase 2
  - Both banks involved in a transaction will be equipped with EPH systems

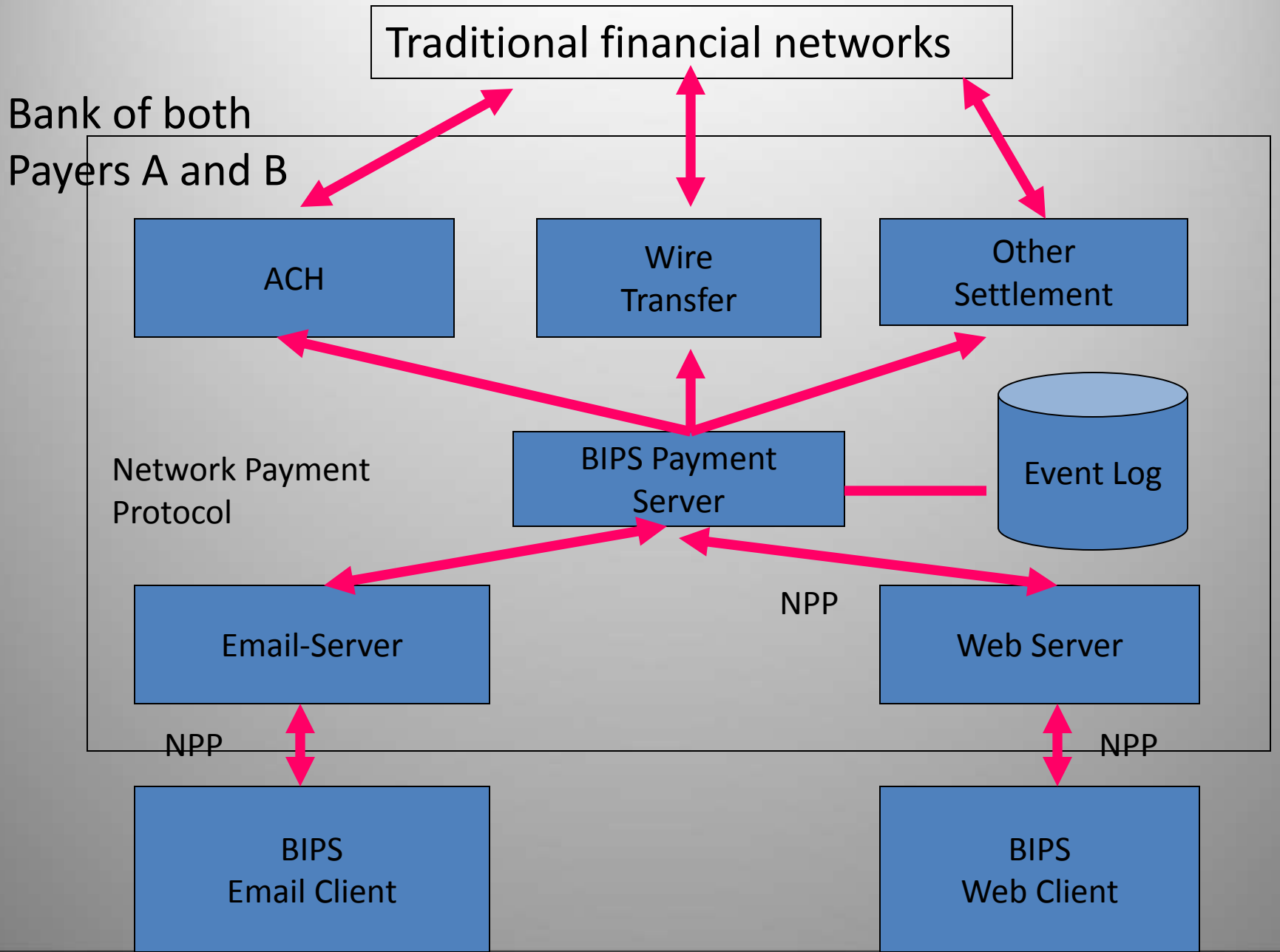
Phase 2 of EPH deployment.



Bank Internet Payment System (BIPS)

- Direct payment methods
  - Credit transfers (giros)
  - ACH payments
  - Wire transfer services
- The BIPS server acts as a gateway to multiple existing bank payment systems
- Protocol for sending payment instructions
- Minimum disruption to existing infrastructure

BIPS architecture



BIPS architecture

- A payer sends (e-mail , Web) BIPS payment instructions to the payment server at the payer’s bank
- BIPS payment server translates the instruction into bank payment transactions

The BIPS protocol functions

- Feasibility request message
- Payment request message
- The status request
- Stop request
  - To cancel an earlier payment instruction
- BIPS server replies with a signed response message

Network Payment Protocol (NPP)

- Defined using the Extensible Markup Language (XML)
- Attribute fields
  - payment type
  - payer and payee details
  - payment amount
- Attributes can be symmetrically encrypted

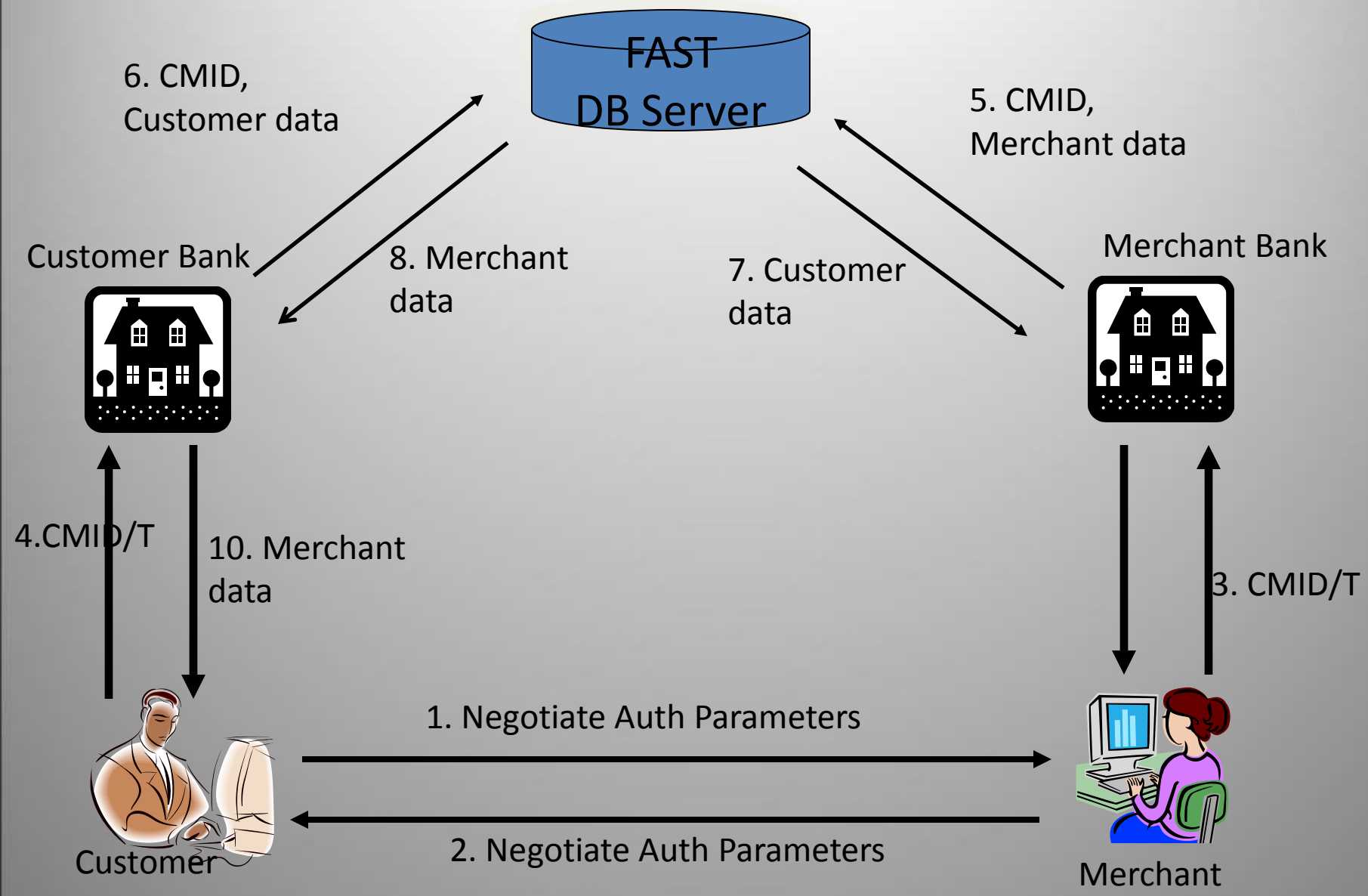
Financial Agent Secure Transaction (FAST)

- A framework for authentication (PKI)
- The PKI are not yet widely deployed
- Banks often act on behalf of parties unknown to each other
- (FAST) project aims to allow banks to provide an identity and attribute verification system on behalf of their customers.

payment guarantee

- checking that
  - A payer has a sufficient bank balance for the transaction
  - The amount is within authorized limits
  - The customer has the authority to commit a company to a purchase.

FAST message flow



FAST message flow

- Steps 1,2
  - The two transacting parties negotiate which identities and properties to verify
  - Consumer Merchant Identifier (CMID)
- Steps 3,4
  - Both the consumer and merchant independently transmit the CMID along with additional transaction information, called the CMID/T, to their own banks.

FAST message flow

- Steps 5,6
  - Each bank sends the necessary information to a FAST database server along with the CMID.
- Steps 7,8
  - The required new information passed back to the appropriate requesting bank.
- Steps 9,10
  - Each bank returns the results to their respective customer who initiated the transaction.

NACHA Internet payments

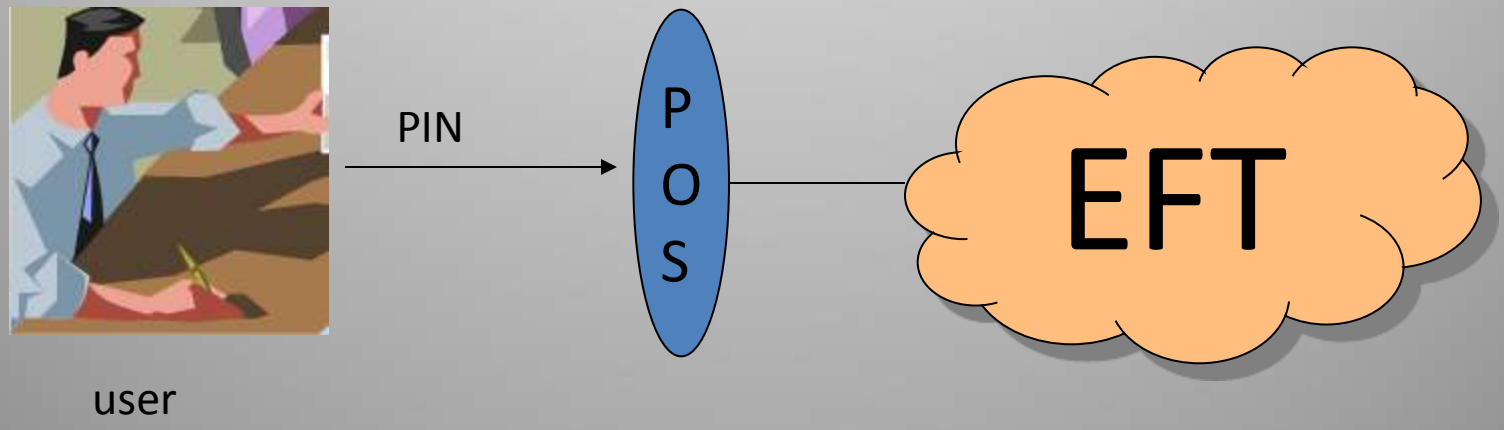
Chapter 5.3

NACHA

- Rules of the use of the ACH network
- Interest of over14,000 financial institutions
- NACHA Internet Council payment projects
  - ISAP: Internet Secure ATM Payments
    - Debit card transactions
  - DirectPay: ACH credit transfer

ISAP: Internet Secure ATM Payments

- Debit cards = ATM cards
- POS: physical point-of-sale
- Electronic Funds Transfer (EFT) network



ISAP

ISAP: Use of ATM cards on the Internet.

- SSL: Internet connection
- Digital signature, instead of a PIN
- Tools:
  - smart card chip (= debit card)
  - smart card reader + wallet software
  - merchant-payment processor

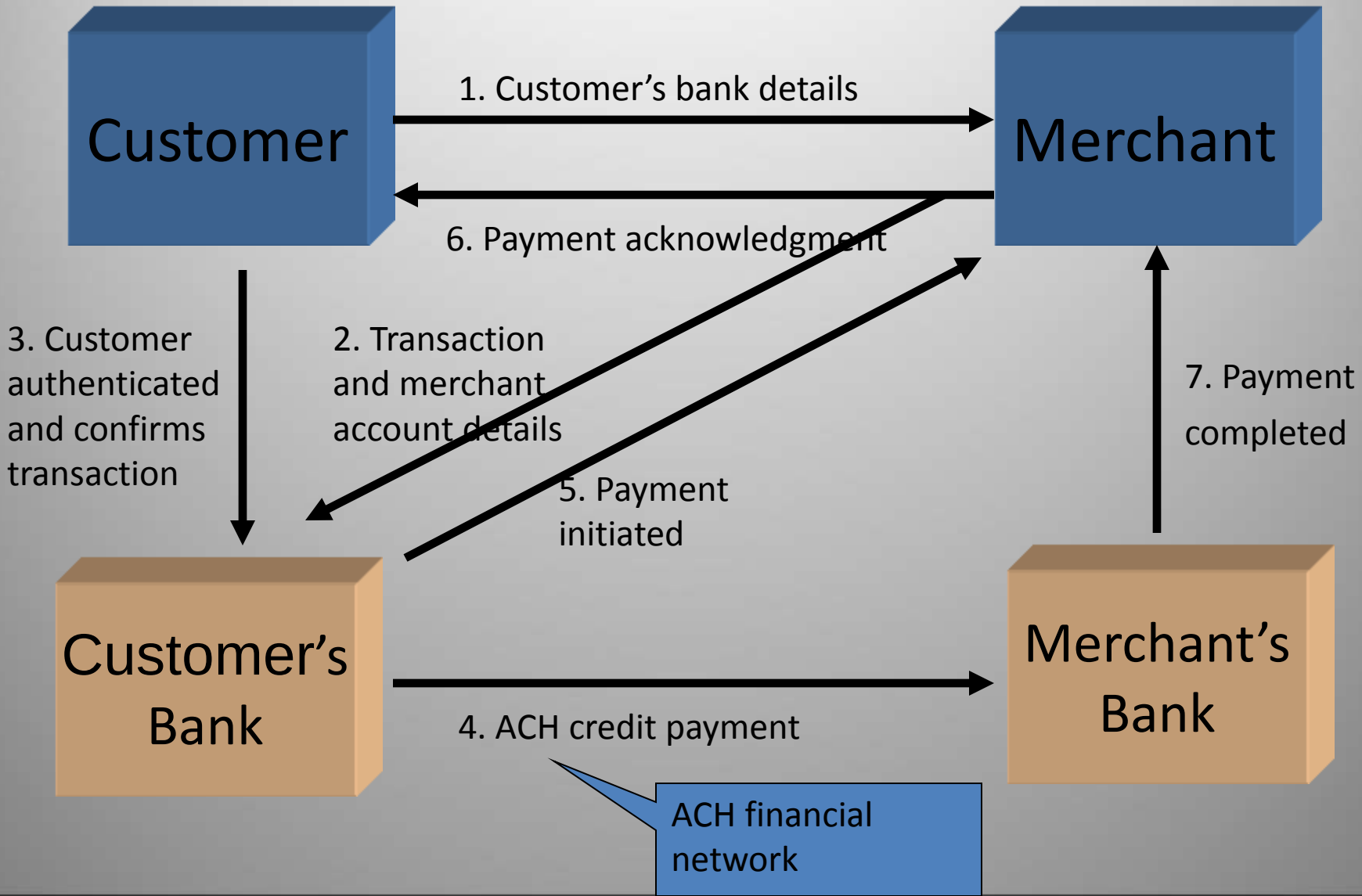
Debit card authorization

- No certificate is required
  - The digital signature is only ever verified at the user's bank, which has a copy of the user's public key already

DirectPay

- Aim of project
  - ACH credits over the Internet
- Previous Models
  - Merchant collects the user's account and bank information, and then performs an ACH debit
- ACH credit Model
  - Initiated directly by the account holder at his or her bank

DirectPay message flow

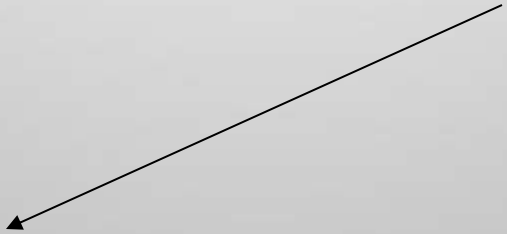


NetBill

Chapter 5.4

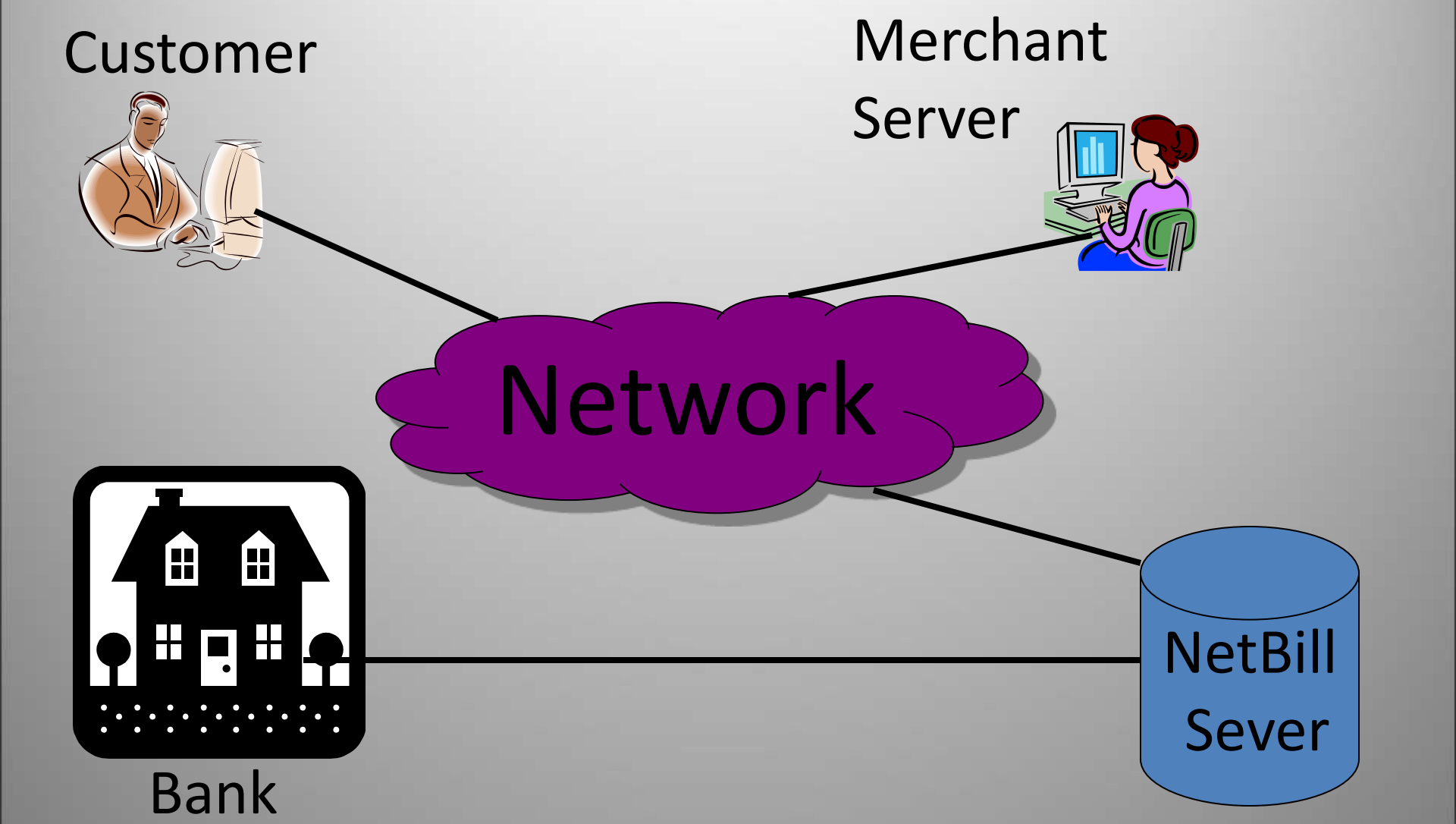
NetBill

- A payment system for the selling and buying of low-priced information goods



Key for encrypted goods

The NetBill concept



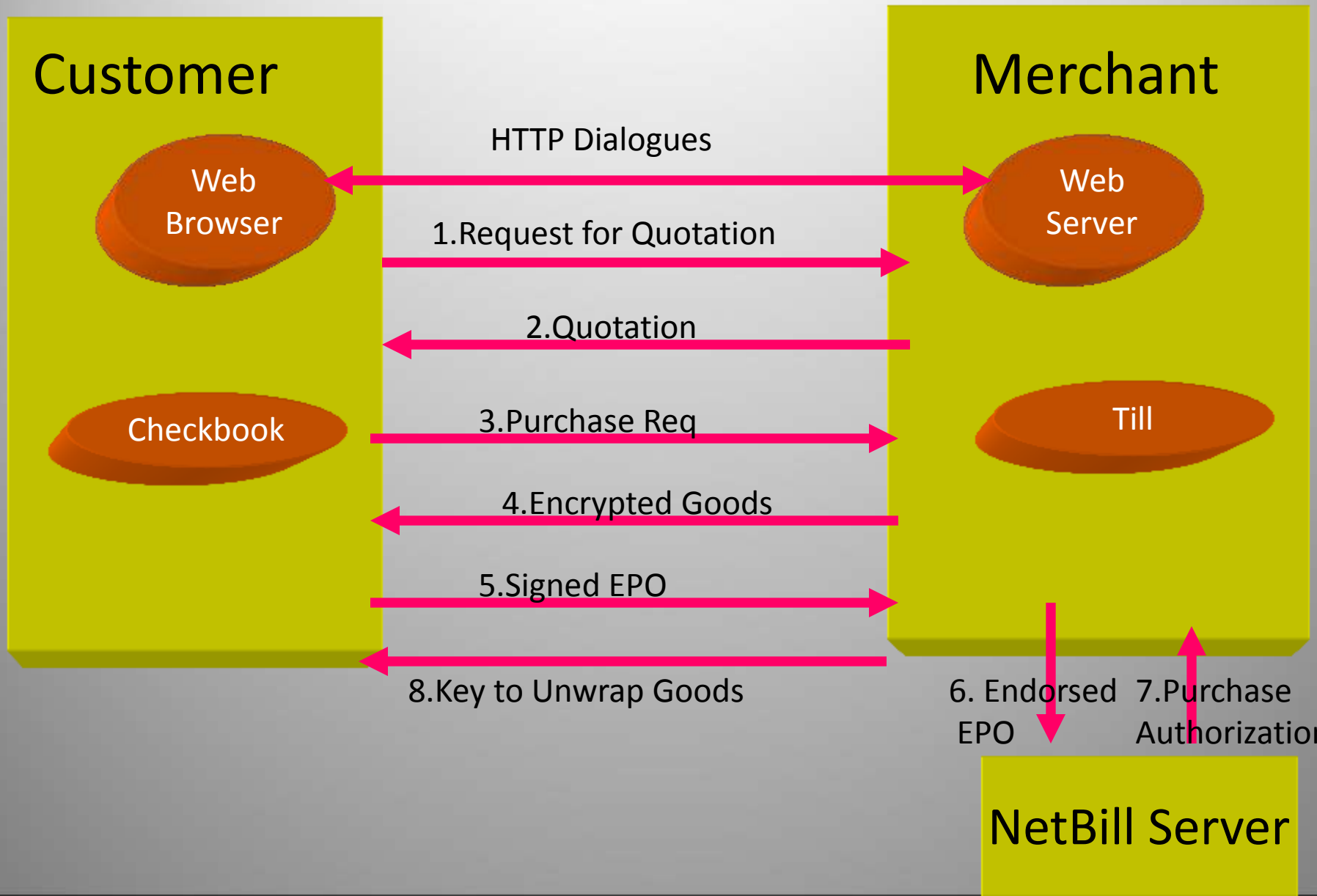
NetBill account

for customer

- Debited for purchases
- Replenished by transferring funds from bank

- for merchant
  - Credited with the value of the goods
  - Deposited into the merchant’s bank

NetBill transaction protocol



- step 1) customer requests a formal quotation
- step 2) merchant determines a price for the user and returns a quotation
- step 3) checkbook sends a purchase request
- step 4) till encrypts goods with a one-time key and computes a cryptographic checksum
- step 5)
  - checkbook: verifies the checksum
  - returns a signed electronic payment order (EPO)
- step 6) till: endorses it and forwards the endorsed EPO to the NetBill server

- step 7) NetBill server
  - verifies that the price, checksums
  - debits the customer's account
  - logs the transaction and saves a copy of the one-time key
  - Returns to the merchant a digitally signed message
- step 8) merchant
  - forwards the NetBill server's reply to the customer's checkbook
  - The key to unwrap the goods

Authentication procedure

- Public Key Kerberos
- A gets the Ticket (T_{AB}) not from a special-purpose server but directly from B

Public Key Kerberos

- A invents a symmetric encryption key, and sends it to B
  - $\mathbf{K}_{\text{OneTime}}$ [**A**, **B**,**TimeStamp**, $\mathbf{K}_{\text{Challenge}}$],
  - $\mathbf{PK}_{\text{B}}$[$\mathbf{K}_{\text{OneTime}}$],
  - $\mathbf{Sig}_{\text{A}}$

Public Key Kerberos

- B constructs a normal Kerberos ticket, $T_{AB'}$ and associated $K_{AB'}$ and returns these to A encrypted with $K_{Challenge}$:

- $K_{Challenge}[T_{AB'}, K_{AB'}]$

NetBill Authentication

- customer ←→merchant
  - establishes T_{CM}
- merchant ←→NetBill server
  - establishes T_{MN}
- customer ←→NetBill server
  - establishes T_{CN}

Transaction protocol

- Customer requests a merchant for a quote for one or more identified products.
- Delivery phase (encrypted goods)
- Customer sends a signed authorization to the NetBill server via the merchant

Price request phase

- customer →merchant
  - T_{CM}, K_{CM}[Credentials, PRD, Bid, RequestFlags, TID]
  - PRD : product request data
  - RequestFlags: give more information on the nature of the purchase
  - TID:transaction ID
- customer ←merchant
  - K_{CM}[ProductID, Price, RequestFlags, TID]

Goods delivery phase

- customer →merchant
  - T_{CM}, K_{CM}[TID]
- customer ←merchant
  - Blinded product
  - K_{Goods}[Goods], K_{CM}[SHA[K_{Goods}[Goods]]], EPOID
  - EPOID :electronic payment order ID

Payment phase

- EPO
  - Details about the transaction
  - Payment instructions (can only be read by the NetBill server)

EPO

- Transaction portion
  - The customer's identity;
  - The product ID and price specified in the merchant's quotation;
  - The merchant's identity;
  - A checksum of the encrypted goods.
- The payment instruction portion
  - A ticket proving the customer's true identity;
  - 'The customer account number;
  - A customer memo field.

Payment phase

- customer →merchant
  - T_{CM}, K_{CM}[EPO, Sig_C]
- merchant →NetBill server
  - T_{MN}, K_{MN}[(EPO, Sig_C), MAcct, MMemo, K_{Goods}, Sig_M]
  - MAcct :merchant.s account number
  - MMemo: memo field

Payment phase

- NetBill server
  - Receipt = [ResultCode, C, Price, ProductID, M, K_{Goods}, EPOID] Sig_N
- NetBill server →merchant
  - K_{MN}[Receipt], K_{CN}[EPOID, CAcct, Balance, Flags]

NetBill server is the bottleneck