© IBM 18.10.96 <wmi@zurich>

Electronic Payment Systems

Michael Waidner

IBM Zurich Research Laboratory
CH8803 Rüschlikon, Switzerland
Ph. +41 1 724 8220 / Fax +41 1 710 3608
<wmi@zurich.ibm.com> / <http://www.zurich.ibm.com/~wmi>

Public Key Solutions 1996
Zurich-Glattbrugg, Switzerland
2 October 1996

© IBM 18.10.96 <wmi@zurich>

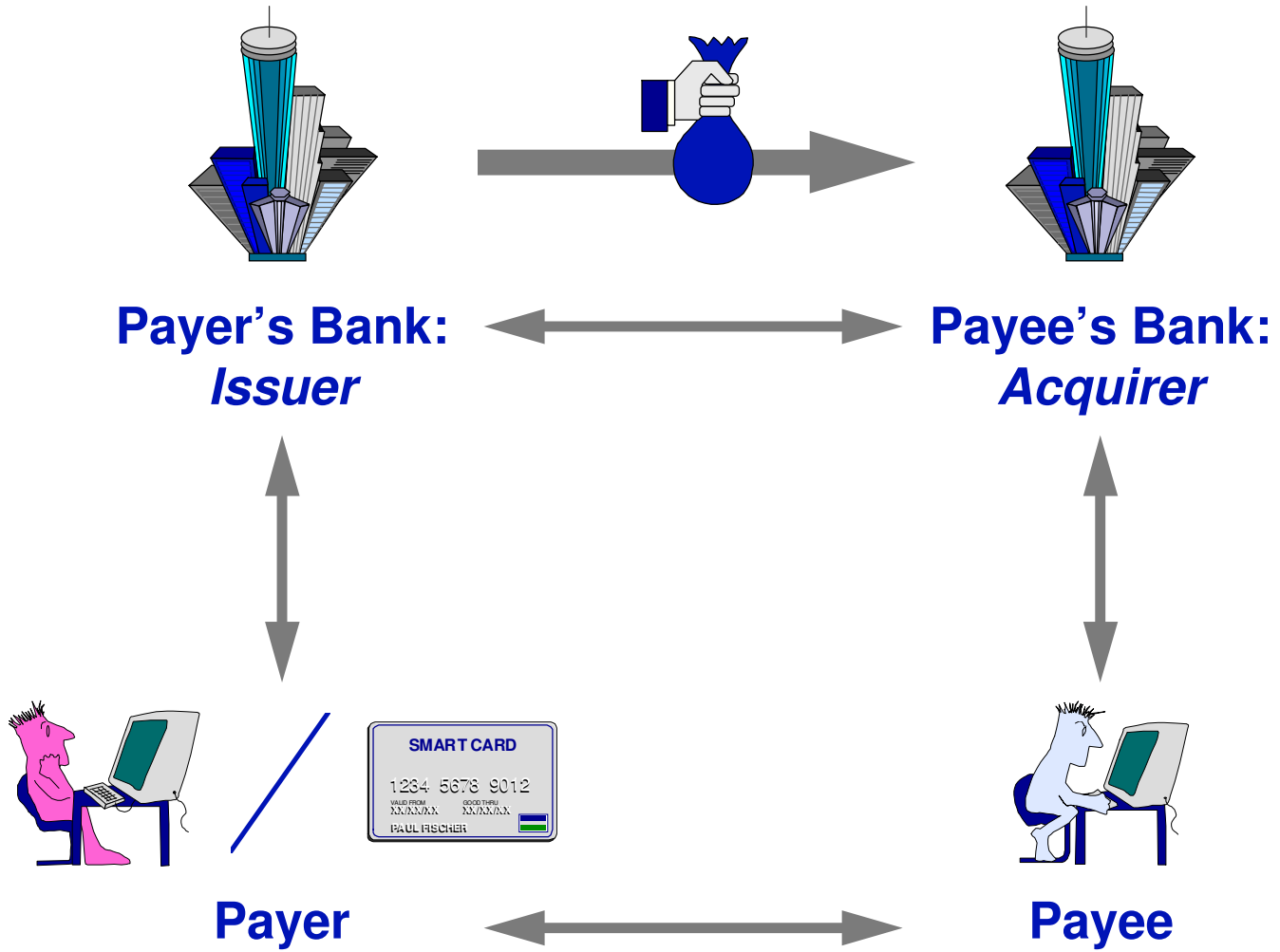
Outline

Outline

- **1. Introduction**
- **2. Security Requirements**
  - Integrity, Privacy, New Requirements
- **3. Security Techniques**
  - Digital Signatures -- Online Creditcards (SET)
  - Tamper-resistant Smartcards -- Offline Purses
  - Blind Signatures -- Untraceable Online Coins
- **4. Existing Systems and Proposals**
- **5. Trusted User Device**
  - Risks, Smartcards and Electronic Wallets
- **6. Summary and Outlook**

© IBM 18.10.96 <wmi@zurich>

What is a Payment System?



© IBM 18.10.96 <wmi@zurich>

What will be Used in the Digital World?

- **The same types as in the paper world!**
  - Cash, for small and anonymous payments
  - Cheques, credit cards
  - Money transfer orders (push, pull)
  - Payment-like systems: vouchers, coupons
- **Same metaphor, i.e.,**
  - same “business model,” same “look-and-feel”
  - at least as cost-effective
  - at least as secure, privacy protecting
  - ... but very different implementation

© IBM 18.10.96 <wmi@zurich>

Payment Integrity

- **Integrity for *payer, payee, payment system***
  - **Nothing happens without authorization**
    - Nobody gives (sometimes also: receives) money without an explicit agreement, stating all necessary payment details
  - **Nothing happens without generating sufficient pieces of evidence**
    - If *X receives* money, it can *prove* this fact to "court"
    - If *X* has *not* given money, nobody can convince a "court" of the contrary
    - Sometimes: If *X* gives money, it gets a *receipt*
  - **The "rules" and technical procedures for "dispute handling" are part of the system!**

© IBM 18.10.96 <wmi@zurich>

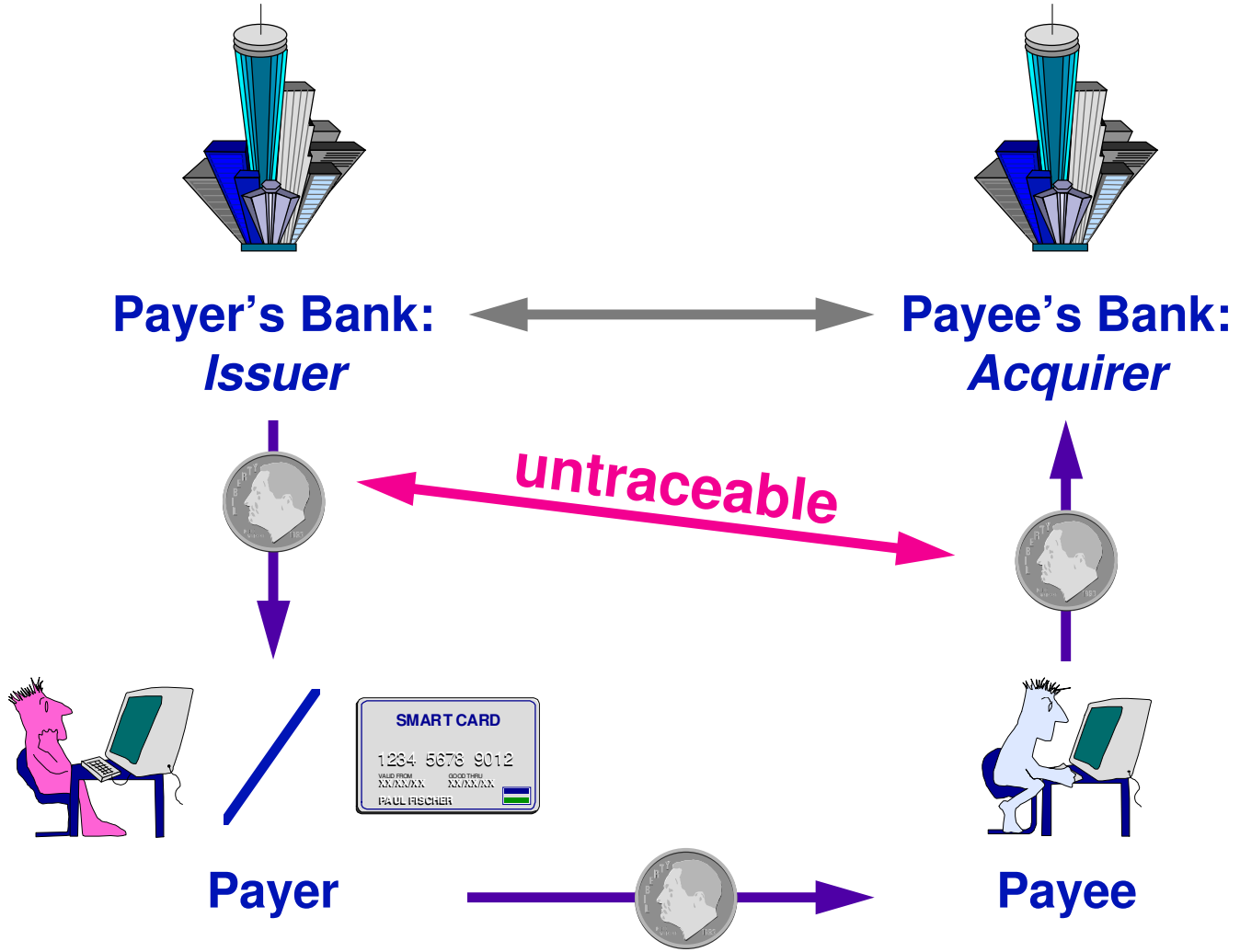
Payment Privacy

- **Privacy of payer and payee**
  - **Payment confidentiality:**
    - Payment details
      - payer, payee, account numbers, amounts, date and time, payment subject, etc.

    must not become known to outsiders
  - **Payment anonymity:**
    - **Payer anonymity:** Only a pseudonym is known to the payee, no identity (*cash*)
    - **Payer unlinkability:** Payee cannot link any two payments of the same payer (*cash*)
    - **Payer untraceability:** Payment system cannot trace payments back to the payer (*coins*)

© IBM 18.10.96 <wmi@zurich>

Payment Privacy (2)



© IBM 18.10.96 <wmi@zurich>

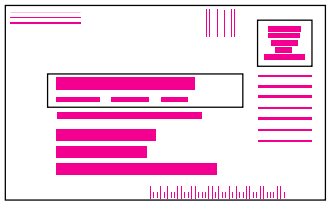
New Security Requirements

- **No negative impact of potential insecurity of digital system on security of paper world**
  - e.g., creditcard numbers must be encrypted
- **Security evaluation!**
  - Payment systems must be **multi-party secure.**
  - No security by obscurity:
    public designs, public evaluations
  - No weak, i.e., no insecure cryptography!
- **Integration into business environment**
  - e.g., link to negotiation and fulfillment
  - e.g., **fair exchange** of *payment / receipt,* or *payment / digital goods*

© IBM 18.10.96 <wmi@zurich>

Internet Security

- **Electronic commerce over the Internet**
  - **Basically *postcard security* only**



  - **Protocols for communication security, like *SSL,* don't address the *payment* problem:**
    - Payments are **multi-party protocols**
    - Just a secure link "buyer -- seller" does not prevent or catch cheating sellers or buyers
    - Non-repudiation requires **"secure documents,"** not just "secure links."

© IBM 18.10.96 <wmi@zurich>

Basic Security Techniques

- **Confidentiality**
  - *strong* encryption
  - "pseudonyms" instead of names
- **Authentication of documents**
  - non-repudiable proofs: digital signatures
  - otherwise (!!!): message authentication codes
- **Double-spending prevention**
  - online database for checking originality
  - physically secure, tamper-resistant hardware

    + copy *detection* after the fact

© IBM 18.10.96 <wmi@zurich>

What's Behind a "Digital Signature?"

- **Mathematical public-key crypto algorithms**
  - ***(secret, public)*** key for ***(signing, testing)***
  - e.g., RSA, DSA, ElGamal + hash function
- **Certification infrastructure:**
  Link between public key and signer
  - What is the "name" of the signer, and how secure is the link between "name" and person?
  - e.g., X509(v3), EDIFACT, EMV '96
  - RA/CA should be **verifiable trusted third parties**
    - secret key only known to owner (or owner's device)
    - registration based on proofs of identity and signed contracts

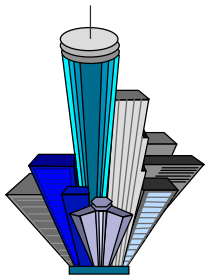
© IBM 18.10.96 <wmi@zurich>

Authentication of Documents

- **For Instance: *Online* Creditcards / SET**

Variants:

- 3KP
- 2KP
- 1KP



© IBM 18.10.96 <wmi@zurich>

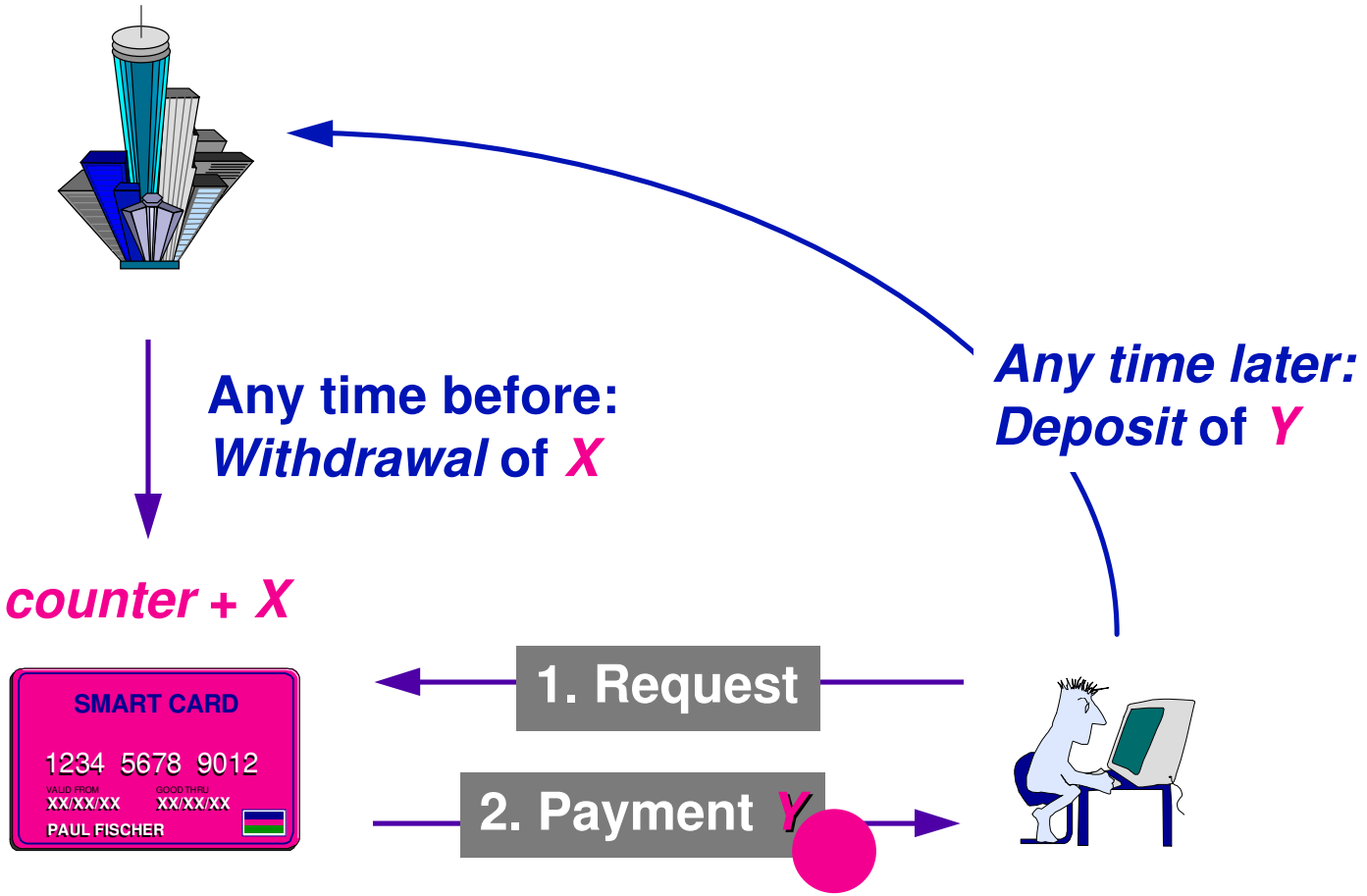
What's Behind a Smartcard?

- **Very small, bankcard-sized one-chip computer**
  - 8-bit Microcomputer, < 5MHz
  - < 512 RAM, 8K EEPROM, 16K ROM
  - ~ 9.6 Kbps IO
  - 0.3 s for 512 RSA signature with co-processor
  - $1 - $10
- **Tamper resistance**
  - **never tamper proof**
  - insider attacks: always possible
  - reading ROM easy
  - reading EEPROM relatively difficult, not impossible

© IBM 18.10.96 <wmi@zurich>

Double-spending Prevention

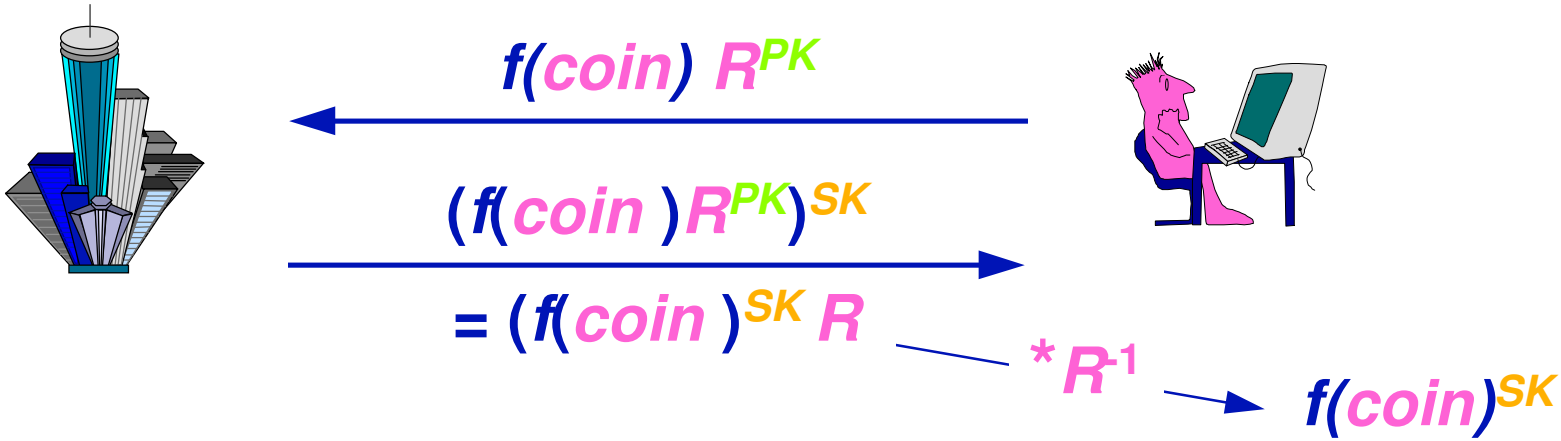
- **For Instance: Signature-based *Offline* Purse**



© IBM 18.10.96 <wmi@zurich>

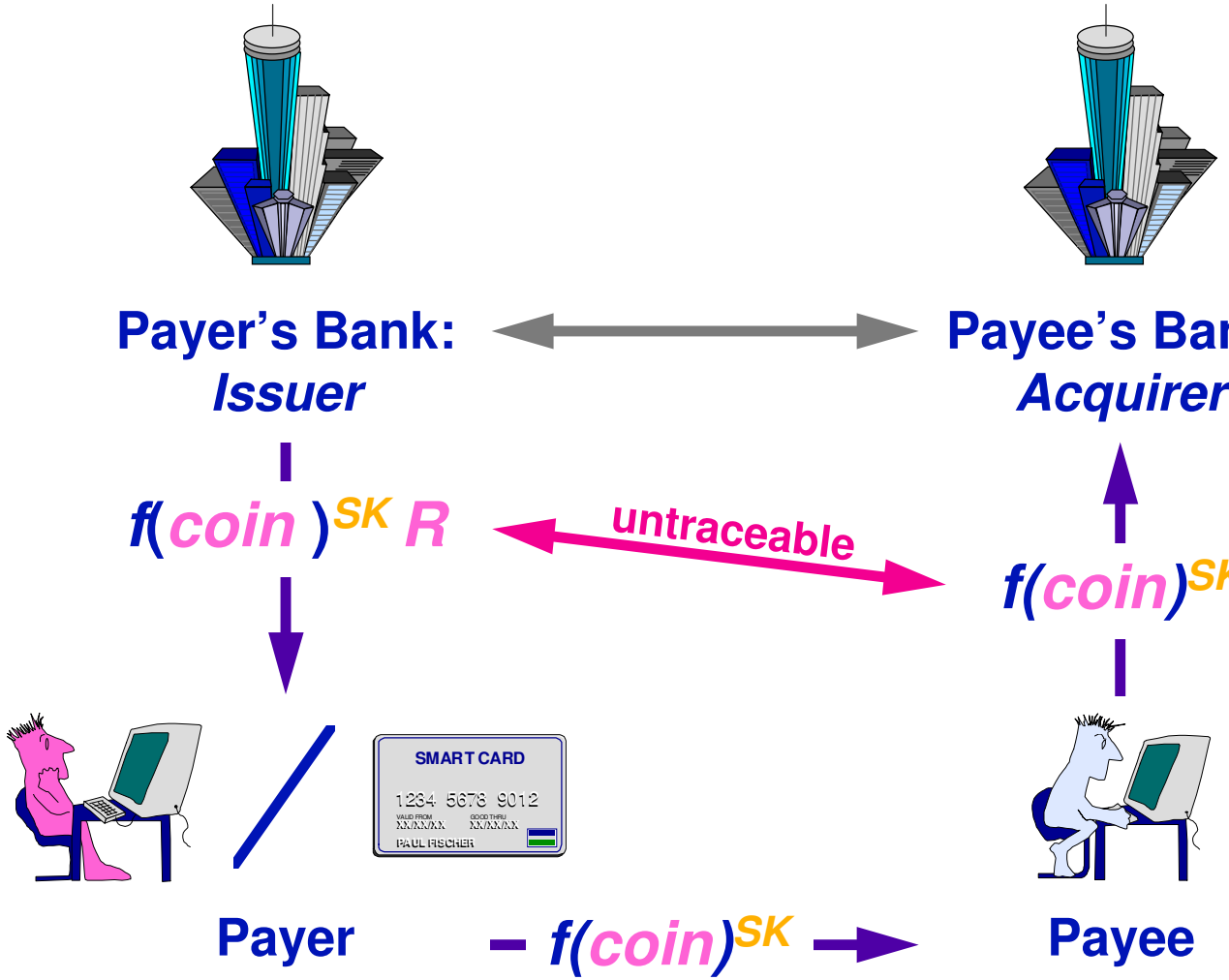
Blind Signatures for Untraceability

- **Untraceable coins: Blind Signatures, e.g., RSA**
  - One-way function *f*
  - RSA pair (***SK***, ***PK***) chosen by **issuer**, defines *one* denomination
  - **Coins: (*coin*, *f*(*coin*)^{SK})**
  - **Withdrawal step**



© IBM 18.10.96 <wmi@zurich>

Blind Signatures for Untraceability (2)



© IBM 18.10.96 <wmi@zurich>

Notions of "Micropayments"

- **Any combination of small amount (0.01 - 10 CHF)**
  - with many **payments in short time,** and/or
  - with payments to **many different payees**
  - e.g., pay-per-click, metered access
- **Problems**
  - policy for implicit user authorization
  - costs for clearing of small payments
  - high frequency / 1 payee: **e.g., CAFE Phone Ticks**
  - high frequency / *n* payees: **e.g., NetBill Server**
  - low frequency: *any system* can be used
- **Not clear yet**
  - economic need for high frequency / many partners

© IBM 18.10.96 <wmi@zurich>

4. Existing Systems and Proposals

	Online Payments	Offline Payments
Traceable	◆ **Crypto-less Systems:** *FirstVirtual + just-do-it* ◆ **Encrypted CC:** *just-do-it, e.g., SSL* ◆ **Secure CC:** *CyberCash, iKP, **SET*** ◆ **Secure Cheques:** *FSTC e-check* ◆ **Billing server for Micro payments:** *NetBill, NetCash* ◆ **Micro payments:** *CAFE Phoneticks, Micro-iKP, Millicent, MicroMint*	◆ **Smartcard-based electronic purses** ◆ **MAC-based:** *Danmont, Proton* ◆ **Signature-based:** ***CLIP*** ◆ *Mondex:* **P-to-P payments, wallets** ◆ **CEN IEP Standard**
Untrace-able	◆ **Anonymous "exchangers":** *Anonymous Credit Cards, NetCash* ◆ **Blind Signatures:** ***ecash***	◆ **Smartcard-based or Electronic Wallets + Blind Signatures:** *CAFE*

+ many other proposals and projects ...

© IBM 18.10.96 <wmi@zurich>

Need for Trusted User Devices

Software-only

Trojan Horse,
Virus

Secret Key
+ Computation
+ Protocols

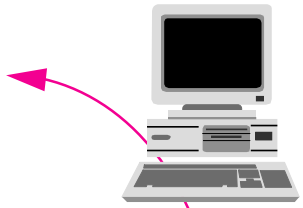
Net

User

Trusted Hardware

Protocols

User

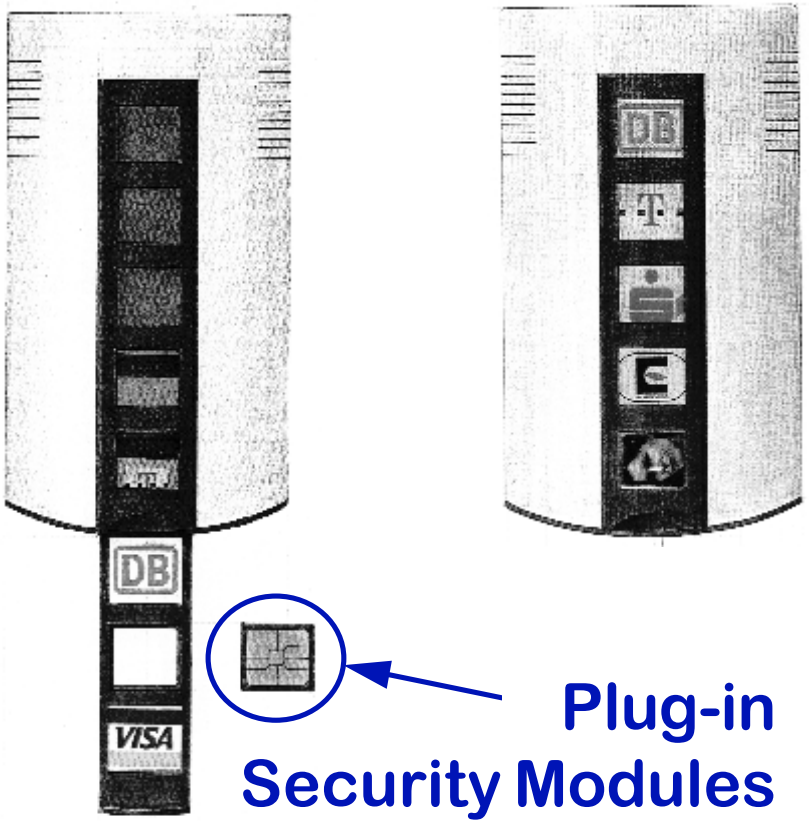


Secret Key
+ Computation
+ Protocols
Wallet

User

© IBM 18.10.96 <wmi@zurich>

Electronic Wallet: *Design Example*



Plug-in
Security Modules

Back

Infrared

Display

Keypad

Front

© N. Özalp, Fachhochschule Hildesheim/Holzminden/Göttingen, 1995

© IBM 18.10.96 <wmi@zurich>

6 Summary and Outlook

- **Electronic Payment Systems**
  - Designs are available, supporting several payment models, multi-party security, privacy
- **Missing Pieces**
  - Public-key infrastructure
  - Secure user devices for high security
  - System integration (architectures, APIs) and negotiation: *projects like SEMPER, JEPI*
- **N.B.: "Payment" is only a small part of electronic commerce!**