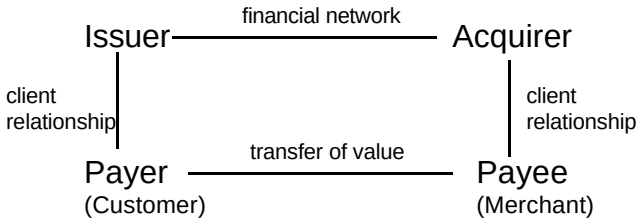
SIEMENS

Table of Contents – 5) Digital Payment Systems

SIEMENS

Mobile Digital Payment Scenario



- Payment: Transfer of monetary value from payer to payee
- Mobile Payment: – ” – via mobile networks
- Mobile Payment Service Providers today
  - Banks / Credit Card Companies / Dedicated Payment Processors
  - Network Operators
    - Identified Customers
    - Prepaid Customers

SIEMENS

Internet Payment Security Technologies

- Plain Security
  - Login & Password, TANs (Transaction Numbers)
- Outband Security
  - Email, mobile phones, premium phone numbers, ...
- Secure Communication Channel (SSL, TLS)
  - Encrypted channel between customer browser & merchant Web server
  - Server authentication, optional browser authentication
  - Supported by the main browsers
- Application Security
  - Digital Signatures
    - Non-repudiation of digital actions
    - Normally wallet support (plug-ins, helper applications, ...) required
    - PKI – Public Key Infrastructure
    - Smart cards for storing the private key
  - Digital Envelopes
    - Encrypting (parts of) messages on application level

SIEMENS

Mobile Payment Security Technologies

- PIN-based Security
  - Authentication and authorization via Login / PIN or Password / TAN
  - Standard security arrangement defaulting PKI based mechanisms
- Mobile Operator Driven Security
  - Channel Encryption between End-User Device and WAP gateway
    - Wireless Transport Layer Security (WTLS)
      - No End-To-End-Security between Customer and Merchant
      - .... unless the Merchant operates the WTLS-Gateway
  - User Identity Module (UIM): (U)SIM/WIM
- Financial Institute Driven Security
  - Dual slot mobile phone – second smart card
  - Multi-application SIM card

SIEMENS

Classification of Mobile Payment Solutions

- Banks / Credit Card Companies / Dedicated Payment Processors
  - Mobile Credit Card Payments
  - Migrating Internet Payment Systems
- Mobile Network Operators
  - Utilization of existing Billing Mechanisms (Prepaid and contract based)
- Multi-Payment Method Frameworks
  - Mobile Network Operators
  - Dedicated Payment Processors
  - Shopping Malls, Large Shops
- Other Mobile Payment Systems
  - Mobile Home Banking, Internet Payments, Mobile Retailer Support

SIEMENS

m-Payment: Market View

Migrating Internet Payment Systems	
CyberCash	Ecash
Geldkarte	IBM-MP
Iti Achat	MilliCent
SET	SSL

Internet Payments With Mobile Phones	
GiSMo	MobilPay
Paybox	Seasoning
WebTrade.Net	Yen-Raku

Mobile Credit Card Payments	
Chargit WAP	EMPS
GMCIG	MasterCard
Netlife	Pure Commerce
Sagem	Trintech
Visa	WireCard

Mobile Home Banking	
724 Solutions	BizPay
EarthPort	PayPal
PostGirot Mob.Smart	S1
Solo e-Payment	W-Trade

Multiple Payment Method Platforms	
Atos Poseidon	Brokat Twister
Ericsson Jalda	GlobeId @Pay
MoreMagic MBroker	PayItMobile
Sonera Mobile Pay	Thyron YES.pay

Mobile Retailer Support	
13Paid	ePayWireless
eXcape	Skypay

Prepaid Accounts
LHS Prepaid
Siemens Pay@Once Prepaid

Other Mobile Payment Systems	
Aether	Mosaic Postilion
Motorola m-Wallet	MovilPago
Telco Italia Easybuy	

* Details in this Lecture * Siemens Involvement

SIEMENS

Table of Contents – 5) Digital Payment Systems

SIEMENS

NetCom Trial – Siemens Pay@Once

- Customer connects to payment center by dialing number displayed on vending machine
- Payment system calls vending machine and informs it that customer can purchase a drink
- When drink is selected, a response is sent to payment center
- Customer's phone bill charged (fixed rate call = cost of refreshment)

SIEMENS

Mobile SET – Secure Electronic Transactions

- Standard by Visa & MasterCard
  - for secure usage of credit cards on the Internet
- Protocols between Customer, Merchant and Payment Gateway
  - Cardholder registration, merchant registration
  - Purchase Request, Payment Authorization
  - Payment Capture
- Uses public-key cryptography
- Credit card companies interested in support of SET by mobile devices
- Today's alternatives to smart cards & advanced security support
  - Server Wallets with Customer Id and PIN authorization
  - Merchant initiated SET in the background, proprietary forms in the front-end
  - Both void the main security feature of SET, i.e. customer non-repudiation

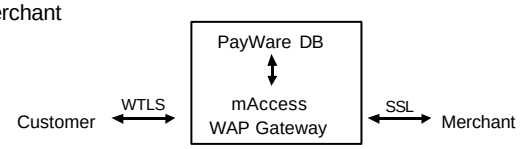
http://www.setco.org
http://www.gmcig.org

SIEMENS

Trintech PayWare mAccess – Form Filling

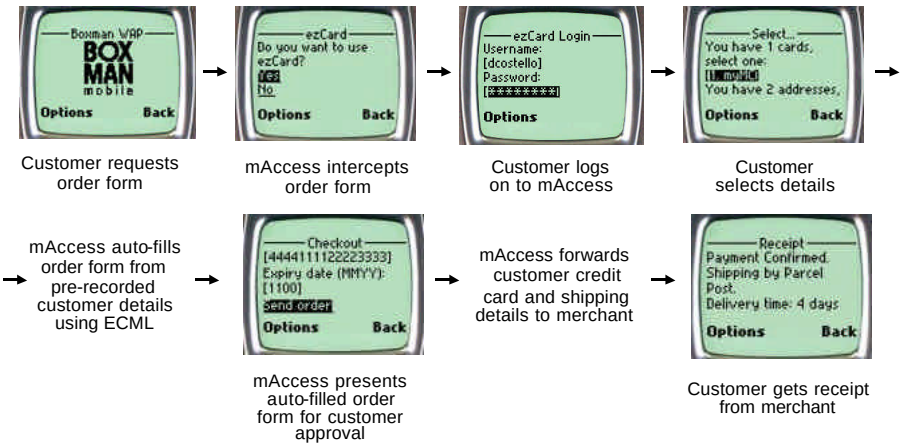
http://www.trintech.com

- PayWare mAccess provides mobile shopping support
  - Pre-recordes customer credit card and shipment address details
  - auto-fills order form using ECML (http://www.ecml.org)
  - transfers payment and shipping details to merchant
- PayWare mAccess operates as protocol monitor
  - kind of WAP gateway / access control proxy
  - monitors communication between customer and merchant
  - authenticates the customer via login and PIN
  - forwards the auto-filled order form to the merchant
- Security
  - WTLS between wireless device and mAccess
  - SSL between mAccess and merchant



SIEMENS

Trintech PayWare mAccess - Workflow



SIEMENS

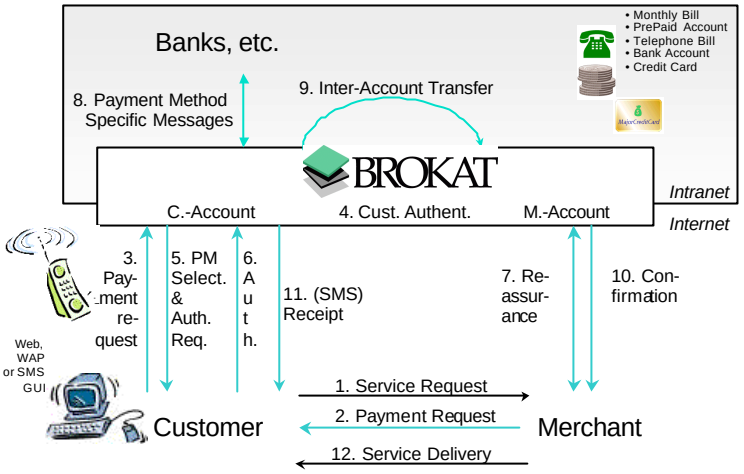
Broker Twister X.Pay

http://www.brokat.de

- The Internet version of Twister X·Pay
  - operationally deployed in many Internet shops and shopping malls
  - small and macropayments
    - credit card payments, account-based aggregation, loyalty points
  - Thin Java Wallet is SET-certified
  - Multi-Payment-Method Broker Framework

SIEMENS

Brokat Twister X.Pay - Mobile Payment Workflow



SIEMENS

Brokat Twister X.Pay - Mobile Payment Screenshots

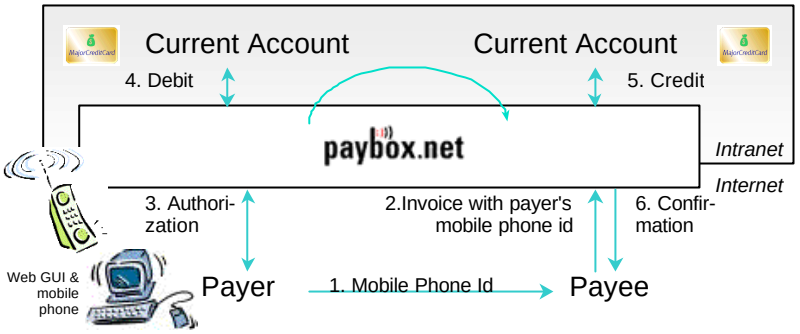
(2/3) Pay Request (5) Invoice (6) Authorization (10.a) Receipt (11) SMS Receipt

- Payment workflows equivalent
  - for the Internet scenario and the mobile scenario
  - allowing for a close integration and an identical merchant payment interface
- Technique of mutual redirections between merchant and broker
  - minimal demands on the customer's end-user device
  - can be handled equally well in WAP and Internet szenarios

SIEMENS

PayBox – Authorization via Cell Phone

http://www.paybox.de



- Customers register with Paybox (mobile phone id and account details)
- Customer renders mobile phone id (1) to merchant, who contacts (2) Paybox
- Paybox calls (3) mobile phone with voice & DTMF based authorization dialog
- Paybox places (4) a direct debit to the customer's account
- Paybox credits (5) and notifies (6) merchant

SIEMENS

PayBox - Further Details

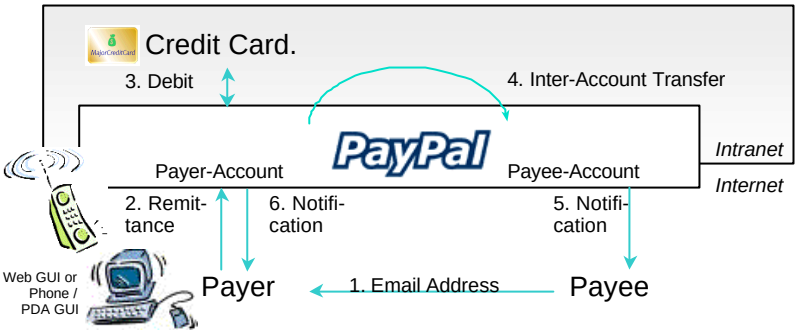
- Peer to Peer / Physical Situation (e.g. Taxi) Mobile Payments
  - TA fee from 25 Cent up to 2 Euro, payment limit 200 Euro
  - Payer renders mobile phone id to payee
  - Payee invoices payer by calling a special Paybox phone number
  - Transaction proceeds as described before
- Security Concerns
  - Payer must render to payee mobile phone Id or Paybox pseudonym
  - These data are sufficient to terrorize the payer with fake invoices
  - Payer uses PIN authentication and authorization
  - Payments neither non-repudiable nor durable
    - Risk for merchant and Paybox operator
- Deutsche Bank involved
- Similar Systems: GiSMo, Seasoning, ...

SIEMENS

PayPal – Mobile Home Banking

http://www.paypal.com

- By Confinity Inc. with support from Nokia and Deutsche Bank
- Peer-to-peer payments via wireless PDAs or Web phones
- From a credit card account to the recipient's PayPal account
- PayPal gains float, customers avoid mailing paper checks
- Access to the user's PayPal account is passphrase / PIN protected



SIEMENS

PayPal – Further Details

- Transaction Workflow
  - (1) The payee places a remittance with PayPal
  - (2) The payment is deducted from the payer's credit card / PayPal account
  - (3) The payment is credited to the payee's PayPal account
  - (4) The payee and (5) payer each receive an email notification
- The payer must register with PayPal
  - New payers must specify their credit card details
- Money can be sent to both PayPal and not yet PayPal users
  - The payer may use a Web-enabled phone or a wireless PDA
  - The payee's email address must be specified
- The payee must sign up or log in to PayPal
  - The payment appears in the payee's PayPal account balance.
  - The payee can transfer the funds to a bank account, request a check, or pay the funds to someone else.
- Similar Systems: EarthPoint, BizPay, ...
  - Use of the mobile phone id instead of email address

SIEMENS

Table of Contents – 5) Digital Payment Systems

SIEMENS

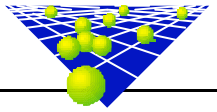
Mobile Payment Systems Summary

- Current Status
  - All systems in very early stages of planning or piloting
  - Usually very little information and technical details disclosed
  - Often little more than declarations of intent
  - Lack of appropriate security mechanisms in the mobile environment
- Indirect payment model dominates
  - UserId / PIN / TAN authentication and authorization widely used
  - Only a few direct payments (e.g. Iti Achat, Geldkarte, ...)
    - Special security support in the mobile end-user device
  - Rarely use of advanced security technologies (e.g. MobilSmart)
    - SIM card application signs SMS remittance authorization

SIEMENS

Mobile Payment Systems Open Issues

- Suitable Security Support in the Mobile Environment
  - Not just UserId / PIN / TAN
  - Strong Public Key Cryptography Based Security Mechanisms
  - Smart Card Support
- Mechanisms Required
  - Ensure: Confidentiality, Integrity, Authentication, Non-Repudiation, ...
  - End-2-End security between customer and merchant
    - Equivalent to SSL, WTLS mostly isn't good enough
  - Mobile Digital Envelopes & Signatures
  - Authentication and WPKI-Support
- Mobile Security and Payment Standardization Bodies (examples)
  - WAP forum: WTLS, E2E-Security, WML Script SignText, ...
  - 3GPP SIM Toolkit standardization
  - GMCIF - MasterCard Global Mobile Commerce Interoperability Forum
  - MSign - Brokat Mobile Digital Signature Merchant API



SIEMENS

Questions and Comments ?

Thanks for your Attention.