Requirements of Commercial Parties

Arnd Weber
IIG Telematics, Freiburg University, Germany
Outline

◆ Types of E-commerce
◆ Threats in E-commerce
◆ Security Tools
◆ Risk Management
◆ How to Secure E-Commerce Economically
◆ Conclusion: Key Requirements
Types of E-Commerce

- **Examples from SEMPER**
  - Mail order-like electronic catalogue sales
  - Sale of information from databases
  - Sales of consultancy
  - ...

- **Other**
  - Banking
  - Contracts
  - Certified mail
  - ...

...
Flexibility Required for Sales

- Different types of documents
  - such as offer, order, receipt
  - with specific data fields

- Configurability
  - different processes
  - steps out-of-band

- Import and export of records
Threats in E-commerce

- **Today**
  - Not getting paid
  - Not getting what was offered
  - Not getting a receipt
  - Loss of confidentiality
  - ... 

- **Increasingly**
  - Fake documents
  - ...

![Image of a worried person with hands out]

![Image of a satellite with a light beam]
Security Tools

- Digital signatures and CA-services
  - Class 1-type
  - French/German rules: I/O
- Encryption
  - SSL long/short keys
  - PGP
- Payments and banks
  - Credit card
  - E-cheque
  - Stored value
- Fair exchange
- ...
Threats with Tools

- **Digital signatures:**
  - Trojan horses
    - Organized crime
  - Eavesdropping of password
  - Relying party losing at court
    - Effect of Trojan horse claimed
  - Impersonated signing party losing at court
    - Insurable?

- **Payments:**
  - Credit card payments may get cancelled
  - Stored value stolen

- **Encryption:**
  - Keys broken/escrowed
Variety of Signature and Certification Services

- Types of registration
  - Personal registration for evidential value
  - On-line registration
  - No registration as with PGP key rings (with paper agreement?)

- Fees for key management
  - revocation
  - statements re validity
  - CLR (privacy)

- Costs for production (incl. certification)
  - software
  - smart cards
  - wallets with secure user I/O
Risk Management Today

- If single value low, for having low damages, sellers
  - check customer databases
  - request paper signature when delivering
  - ask for payment
    - Cash on delivery
    - Credit card
- If single value is high or likelihood of damage high, buyers and sellers don’t do electronic commerce
Risk Management Tomorrow

- If single value is low, and damages increase
  - players will use digitally signed documents
  - sellers will ask for irrevocable payment
- If single value is high or likelihood of damage high
  - players will use digitally signed documents
  - players will use fair exchange for value against receipts
- If players use digital signatures, will new risk of perfect impersonation emerge?
How to Secure E-Commerce Economically?

Types of E-Commerce

- Examples from SEMPER
  - Mail order-like electronic catalogue sales
  - Sale of information from databases
  - Sales of consultancy
  - ...

- Other
  - Banking
  - Contracts
  - Email
  - ...

Security Tools

- Digital signatures and CA-services
  - Class 1-type
  - German Signature Law

- Encryption
  - SSL long/short keys
  - PGP

- Payments
  - Credit card
  - E-cheque
  - Stored value
  - ...

...
Economically Efficient Usage of Tools I

- Freedom of choice of tools
  - Players make cost/benefit analysis when selecting a tool
  - Players have to adhere to different legal settings
  - Players want competition between providers of tools
- Usability of tools for different business processes
- Low costs for adaptation of business applications and tools
- If business application integrated into other systems: no need to modify adaptation for new tools
Economically Efficient Usage of Tools II

- Usability by everybody
- Single way to negotiate protocols
- Support of forms
  - for transfer of information between document types
  - for verification of content
  - for language support
Economically Efficient Usage of Tools III

- Legal certainty achievable

- Limitation of possible damage must be possible
  - loss of house, prison

- Openness for fair behaviour
  - e.g. signed offers, receipts

- Single user interface for tools and management of keys
**Conclusion: Key Requirements**

- **Economic to have for all users:**
  - integration of tools only once
  - choice of tools as secure and fair as requested
  - integration of business applications only once
  - single way to negotiate protocols
  - single user I/O
  - transfer of information from document to document
  - verification of contents of documents
  - isolate backend from tools

- **Options to be selected by users:**
  - one legal framework for non-repudiatable documents, with option for liability limit
  - services for signing, payment, encryption, fair exchange
  - business processes
  - types and fields of documents