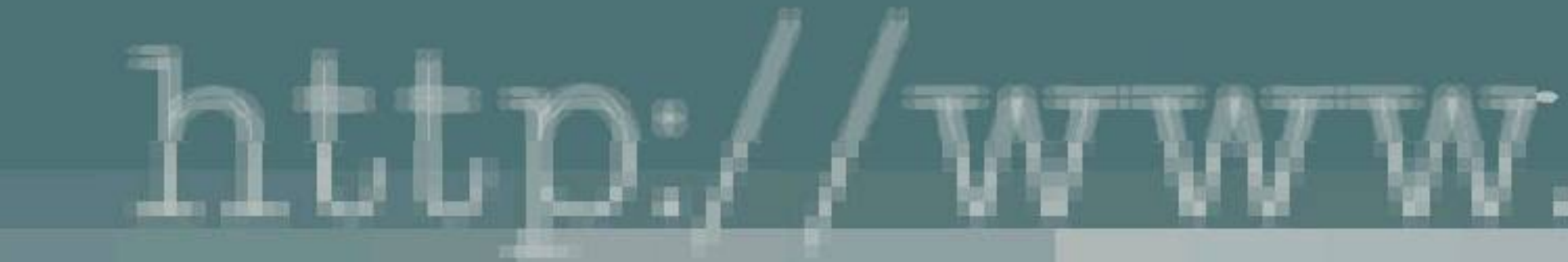
E-Commerce Security: A Primer

John Iliadis

jiliad@aegean.gr

Presentation Outline

- Introduction to E-Commerce
- Enabling E-Commerce through Security
- A Short Primer on Information Security
- Confronting with E-Commerce Threats
- A Survey of E-Payment and M-Payment Systems
- Case Study: ATM Fraud



Introduction to e-Commerce

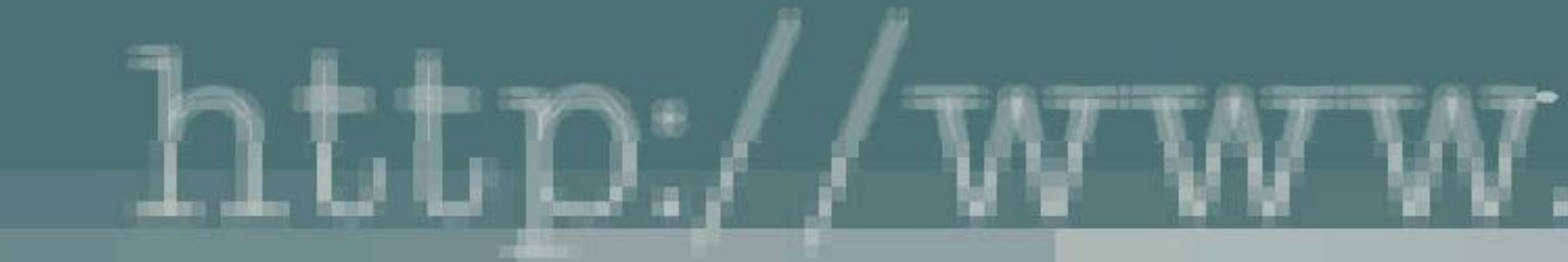
E-Commerce: Business and Technology Innovation

E-commerce introduces new methods in:

- Communications
- Business Transactions
- Market Structure
- Education
- Work

E-Commerce Pros

- Fast and easy access to information for individuals
- Reduces costs
- Opens up new markets
- Increases competition
- Lowers prices



E-Commerce Cons

- Cyberspace is anarchic
- E-commerce also reduces costs for fraudsters
- It retracts the trustful nature of business which we were used to practice
  - Contracts,
  - Invoices,
  - Person to person contact,
  - Existing legal framework for doing business
- "Digital divide" cultural, gender and race gap in the use of Internet)

Adoption of E-Commerce in Greece

- 38% of the participant companies use electronic commerce practices
  - 12.5% integrated e-commerce to their business
  - the rest 25.5% are opportunistic users of e-commerce

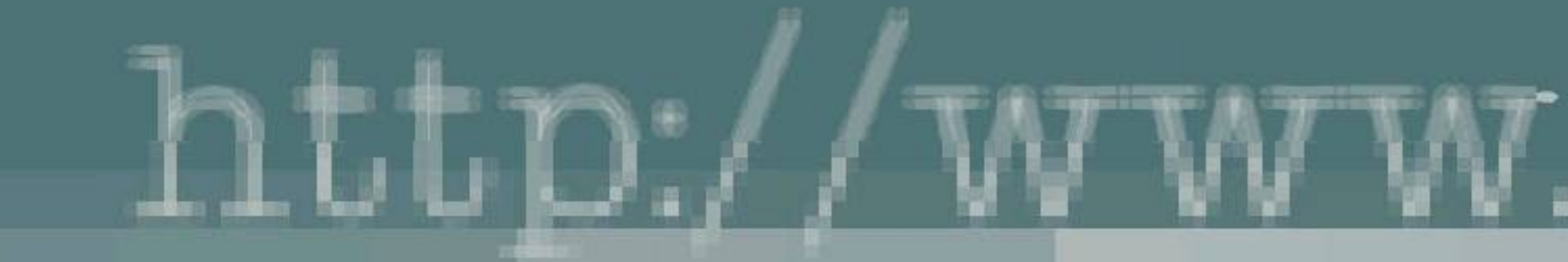
- 47% of the companies are planning to adopt electronic commerce while the 33% of those are planning to do so within the next year.

Study by ELTRUN, AUEB, Greece (2001); statistical sample: 240 Greek companies

E-commerce & Trust

What is Trust?

- Trust allows us to reasonably rely on the information or actions of another party.
- Trust is an intrinsic and subjective property which may be propagated but not transferred



E-Commerce & Trust (2)

Trust in traditional commerce environment

- Contracts, invoices, person to person contact, existing legal framework for doing business in a trustful manner

Trust in e-commerce

- No apparent legal framework, at least for B2C commerce; under development
- Distant transactions between unknown parties
  - Lack of identification, the way customers were used to practice it
  - Lack of authentication, the way customers were used to practice it

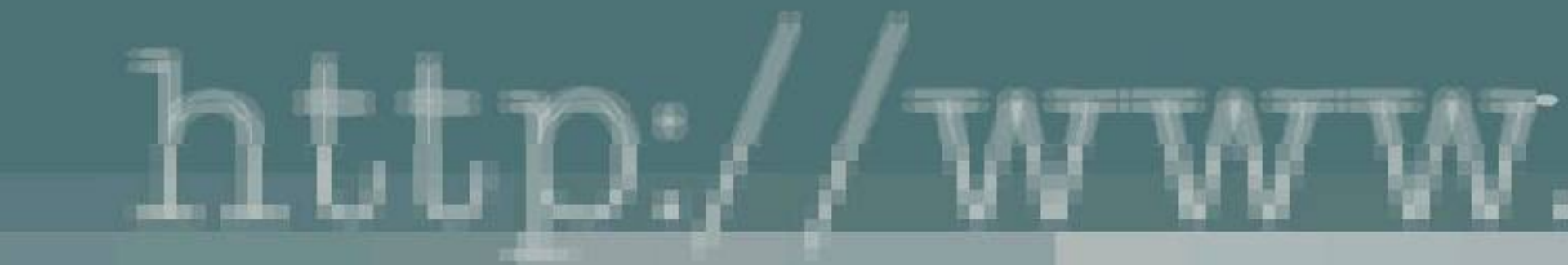
Inherent Need for Trust

- The need for maximising trust is inherent, because trust enables business, but…
  - More Trust = More Risk
- We need to analyse and manage the risk (eliminate, accept or transfer the risk)
- Risk Management is well understood in contemporary organisations

Enabling E-Commerce through Security

Management Decisions & Risk Analysis

- There is no 100% security
- Need for a solution that balances cost and security requirements
- Information Security is not a hindering factor, it is an *enabler*

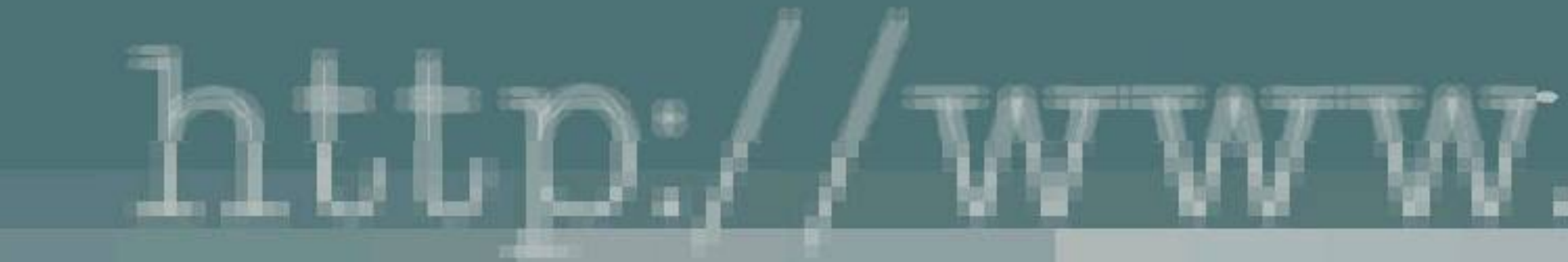


Costs of Information Security

- Implementation costs
- Costs of incorporating procedures, services and mechanisms to existing systems
- Costs of deploying new procedures, services and mechanisms
- Functional costs
  - Hardware
  - Software
  - People
  - Change Management
  - New Business Processes

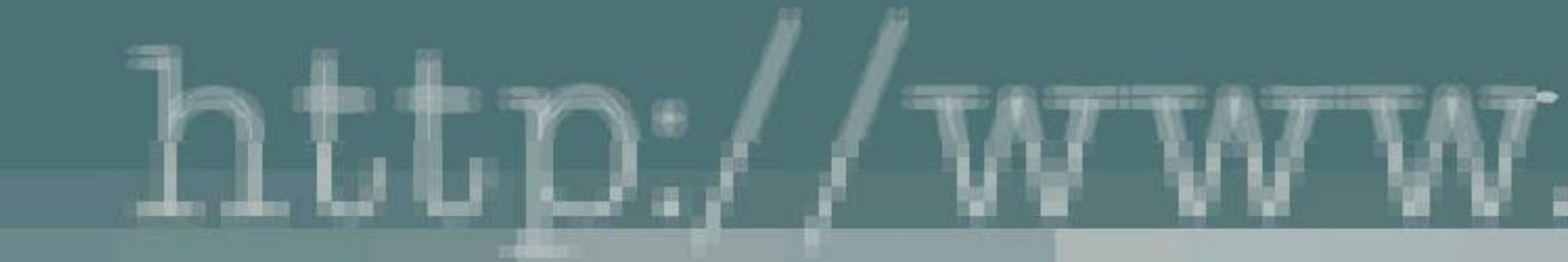
Where do Security Requirements come from?

- Risk analysis, based on
  - Existing business processes
  - Interviews with company executives
  - Legal issues (e.g. privacy laws)
  - Corporate image
  - Potential enemies (likelihood of a security attack)



Security Life-Cycle

- Risk analysis
- Security policy
- Overall system re-engineering
- Security management of deployed system
- Incident Response
- Business Continuity Planning



Risk Analysis!

What is at risk
- Qualitative analysis
- Quantitative analysis

What vulnerabilities can be exploited
- Technical
- Process
- People

Risk management
- Eliminate/reduce risk
- Accept risk
- Transfer risk

Managing risk becomes part of the everyday business process

Information Security Policy

- The basis for all information security efforts
- Directs how issues should be addressed and technologies used
- The least expensive control to execute, but the most difficult to implement
- Shaping policy is difficult because policies must:
  - Never conflict with laws
  - Stand up in court, if challenged
  - Be properly administered

Need for E-Commerce Security

- The number of cyber attacks skyrocketed from approximately 22,000 in 2000 to over 82,000 in 2002
- First quarter of 2003 the number was already over 43,000

Source: US Computer Emergency Response Team (US CERT)

A Short Primer on Information Security

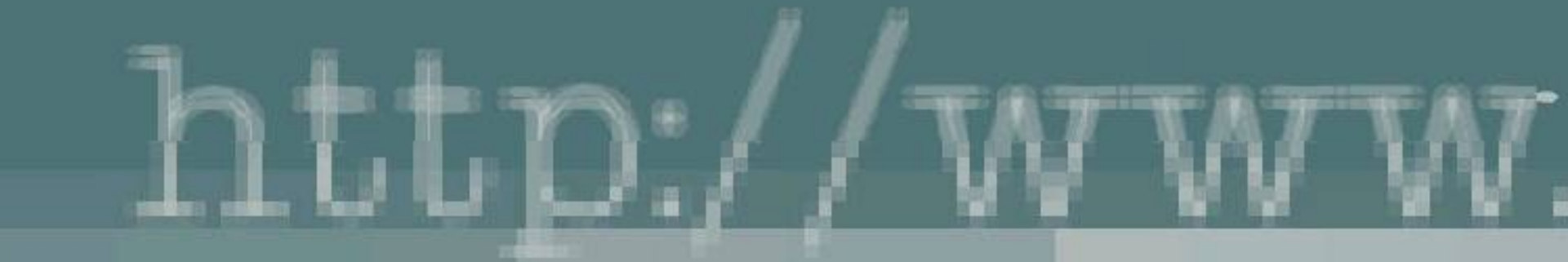
A Short Primer on Information Security

- …it is not about technology, or at least not only about technology
- It is about building Information Systems in a way that *risk is being managed (eliminated, accepted, transferred)*

- Basic Information Security properties: CIA
  - Confidentiality
  - Integrity
  - Availability

…more Information Security services

- Authentication: verification of one's identity
- Access Control: control over what information or resources can be accessed by specific people
- Non-repudiation: the inability to deny having done something (e.g. sent an email, received an email, digitally signed stg, etc)
- Privacy: confidentiality of personal information
- Anonymity: confidentiality of identity



Challenges for Information Security

Information Systems

Then

- Centralised, Closed,
- private or semi-private, no access allowed,
- wide spectrum of proprietary networking/communication protocols,
- expensive,
- targeted user group,
- early Internet instances.

Now

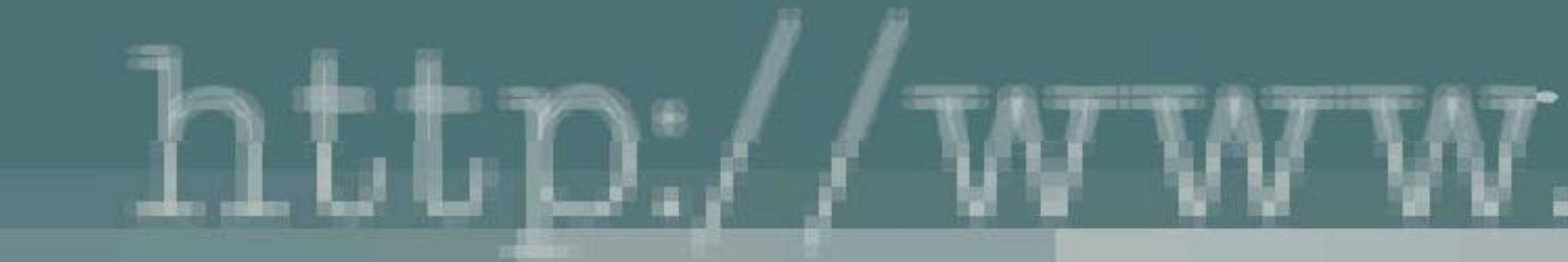
- Distributed, Open,
- no ownership,
- no central control,
- resilience,
- access to anyone,
- standardised protocols,
- Internet access,
- low-cost access.

Some General Principles

- Security must have a total approach—you're only as strong as your weakest link
- The risks do not only stem from external sources; most of the times, they stem from internal sources (e.g. disgruntled employees)
- Security is not a cousin of Obscurity ("… the only good locks are open, public and accessible ones", W. Diffie)

Bottom Up Approach to Security

- Systems' administrators attempting to improve the security of their systems
- technical expertise of the persons involved
- Seldom works since it lacks critical features:
  - Management support
  - Employees' support



Top-down Approach to Security

Initiated by higher-level management:

- Issue policy and procedures
- Dictate the expected outcomes
- Determine who is accountable for each action

Advantages:

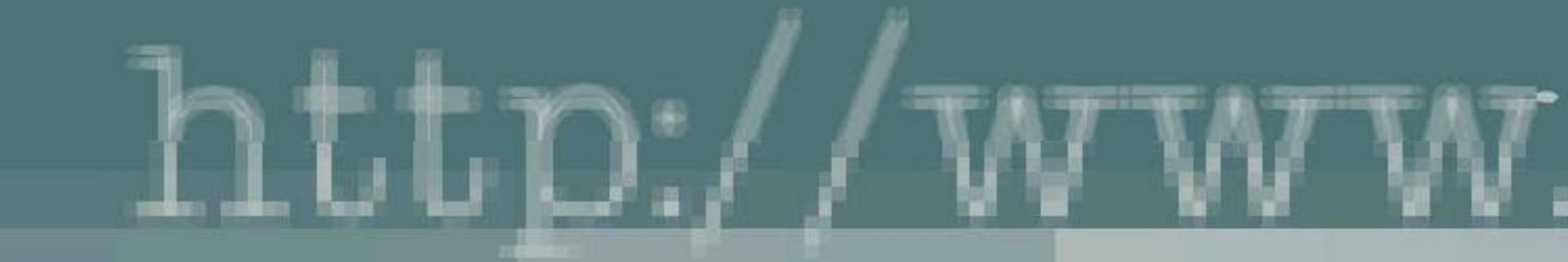
- Strong management support
- Dedicated IT personnel
- Dedicated funding
- Clear planning
- Support from employees

Security Project Team

- Chief Security Officer
- Chief Information Officer
- Risk assessment specialists
- Security administrators
- Security engineers
- System administrators
- End users (!)

A Short Introduction to Cryptography

- Symmetric Cryptosystems
- Asymmetric Cryptosystems
- Digital Signatures



A Short Introduction to Cryptography: Symmetric Cryptosystems

Alice

Symmetric key: "pass21"

ENCRYPT

document

Encrypted document

Network

Network

Bob

Symmetric key: "pass21"

DECRYPT

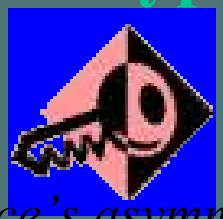
Encrypted document

A Short Introduction to Cryptography: Symmetric Cryptosystems

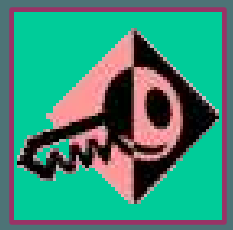
- Both Alice and Bob have the same key (pass21)
- *Encryption/decryption:*
  - Step 1: Alice encrypts the *document* with key "pass21" and sends to Bob (e.g. over e-mail) the *encrypted document*
  - Step2: Bob receives (e.g. e-mail) the *encrypted document* and uses key "pass21" to decrypt it and retrieve the original *document*
- Alice has got to communicate to Bob the key ("pass21") in a secure manner, i.e. no one else must know what they key was (mail?).

A Short Introduction to Cryptography: Asymmetric Cryptosystems

Alice



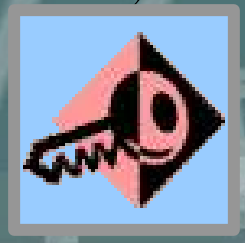
Alice's asymmetric PUBLIC key "pert35"



Alice's asymmetric PRIVATE key "proe34"

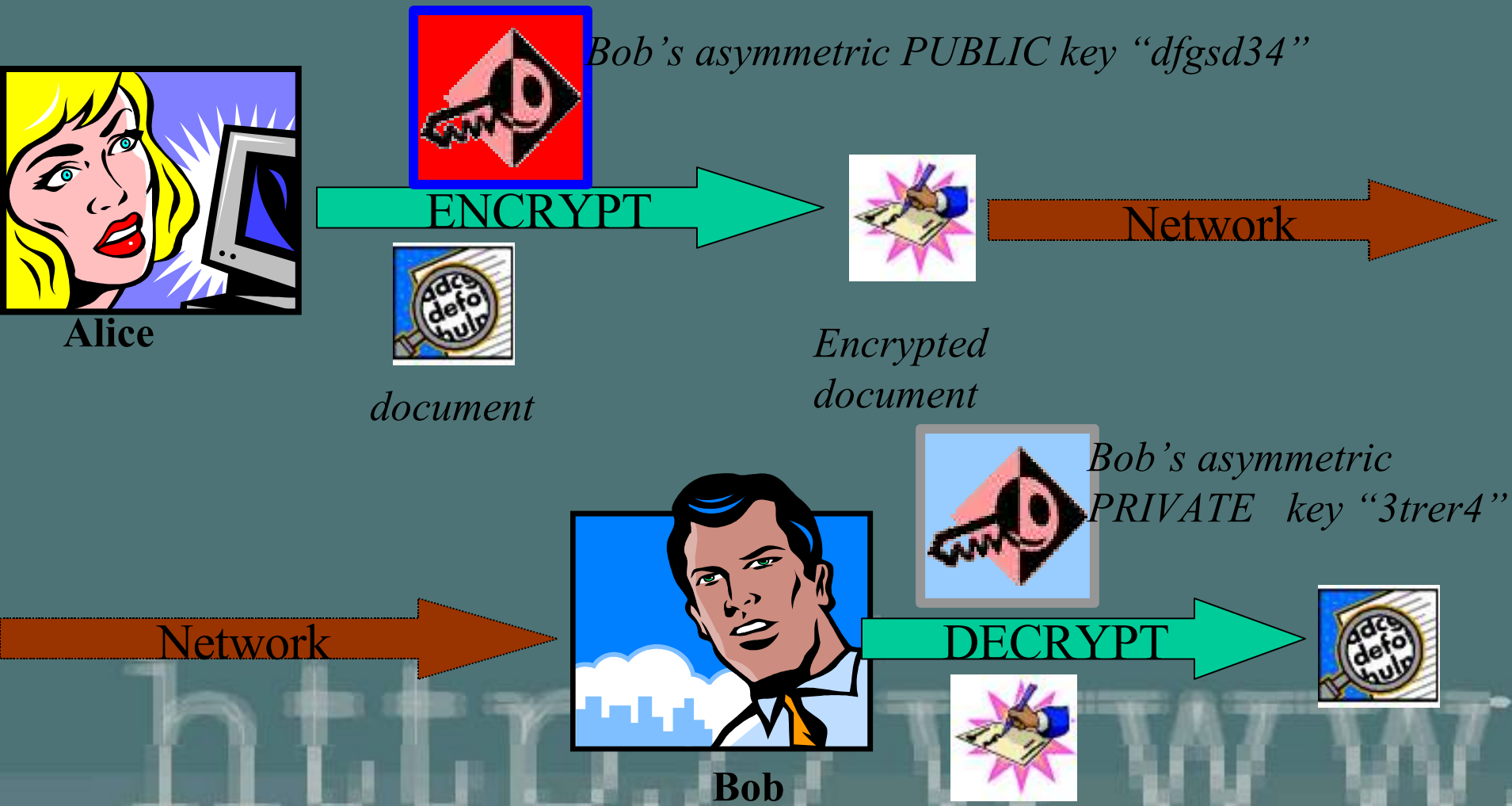
Bob

Bob's asymmetric PUBLIC key "dfgsd34"



Bob's asymmetric PRIVATE key "3trer4"

A Short Introduction to Cryptography: Asymmetric Cryptosystems



A Short Introduction to Cryptography: Asymmetric Cryptosystems

- Alice has a public and private keypair
- Bob has another public and private keypair
- *Encryption/decryption:*
  - Step 1: Alice encrypts the *document* with Bob's public key "dfgsd34" and sends to Bob (e.g. over e-mail) the *encrypted document*
  - Step2: Bob receives (e.g. e-mail) the *encrypted document* and uses his private key "3trer4" to decrypt it and retrieve the original *document*
- Bob has got to communicate to Alice his public key ("dfgsd34") in a secure manner, i.e. no one else must be able to tamper with the key (mail?).

Symmetric versus Asymmetric Cryptosystems

- Symmetric cryptosystems
  - they involve the use of one key only, shared between A(lice) and B(ob),
  - this key must be confidential, i.e. known only to A(lice) and B(ob).

- Asymmetric cryptosystems
  - they involve the use of a keypair (public+private key) for each party, i.e. Alice has a public and a private key, while Bob has his own public and his own private key,
  - Bob's public key must be made known to Alice in a way that Alice can be sure that the integrity of Bob's public key has not been violated.

Digital Signatures

Alice

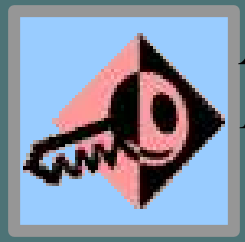
Alice's asymmetric PRIVATE key "3trer4"

SIGN

document

Signed document

Network



Alice's asymmetric PUBLIC key "dfgsd34"

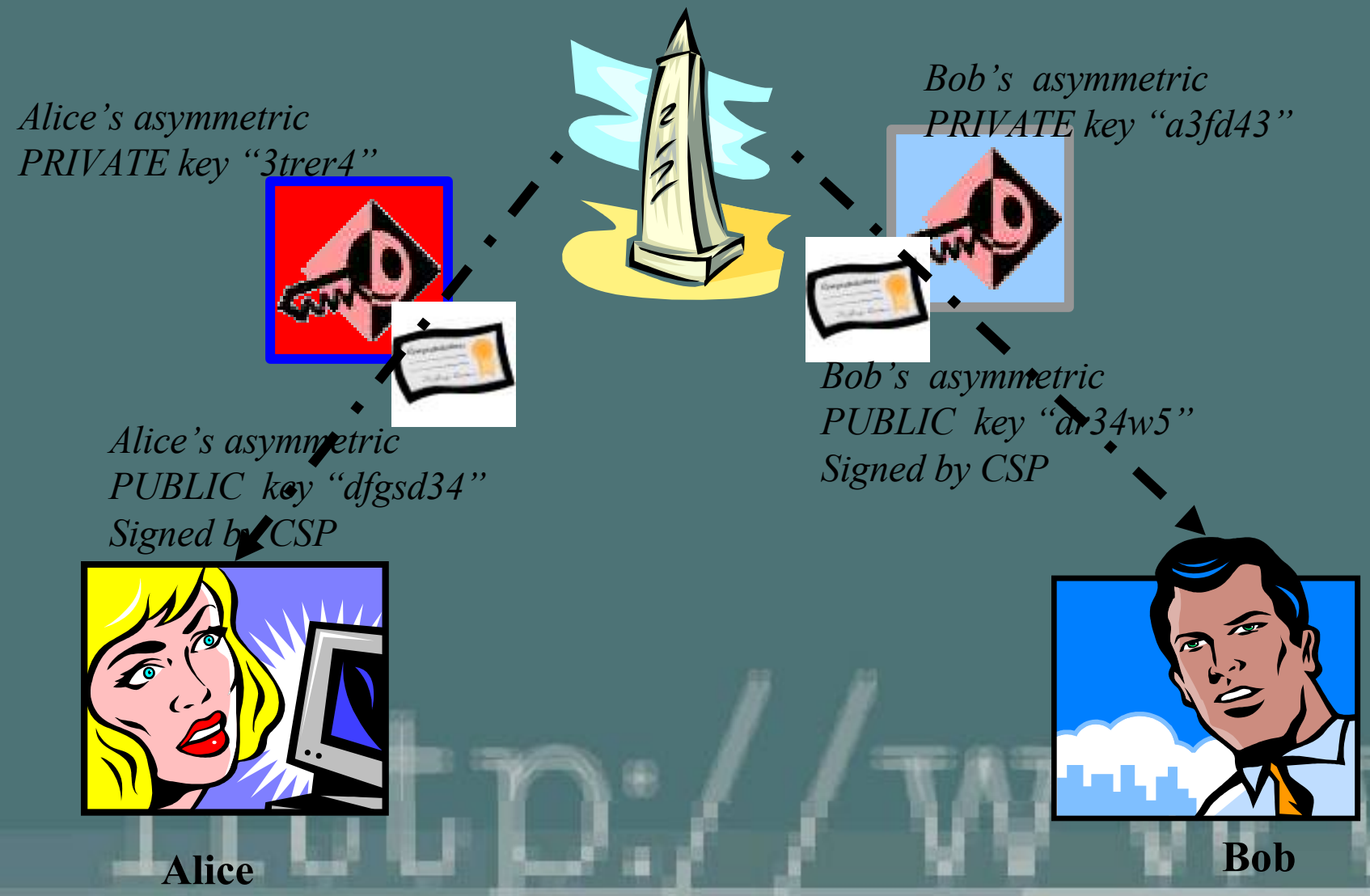
Network

Bob

VERIFY SIGNATURE

Signed document

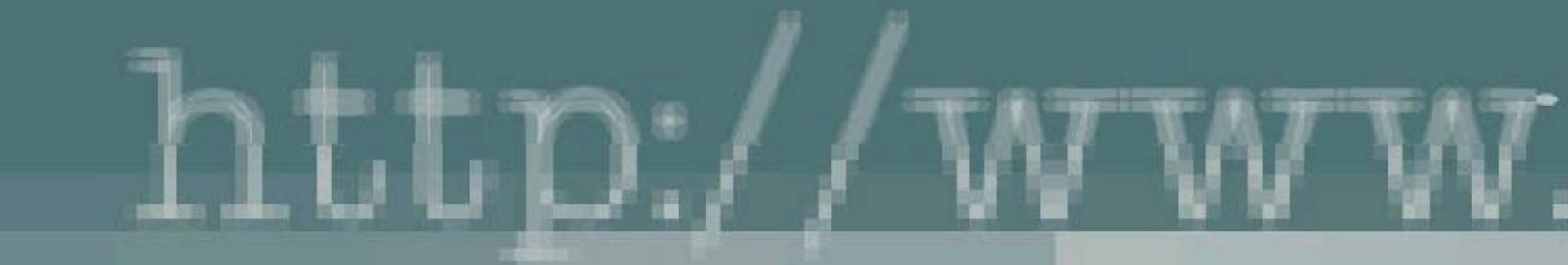
Certification Service Provider



Confronting with E-Commerce Threats

Some Threats in Electronic Transactions

- Monitoring of communication lines
- Shared key guessing
- Shared key stealing
- Unauthorised modification of information in transit
- Masquerade - Web spoofing
- Password stealing
- Unauthorised access



Insecure Electronic Transactions

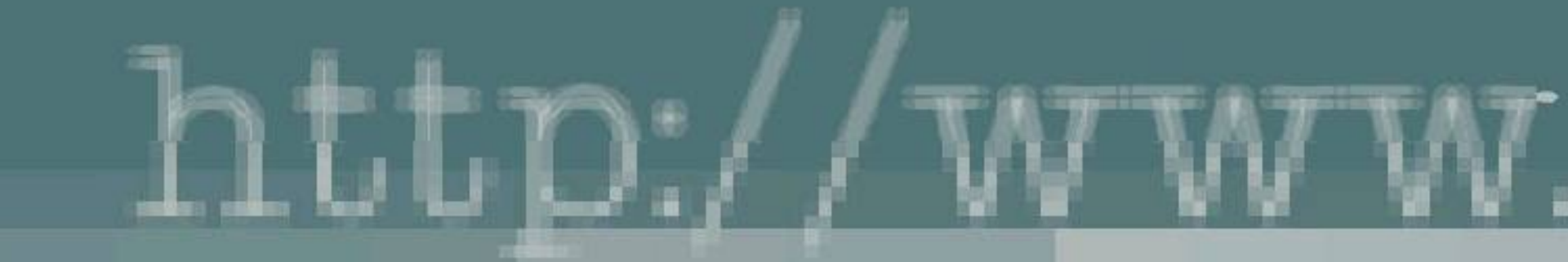
insecure communication channel

Facing Threats using Cryptography

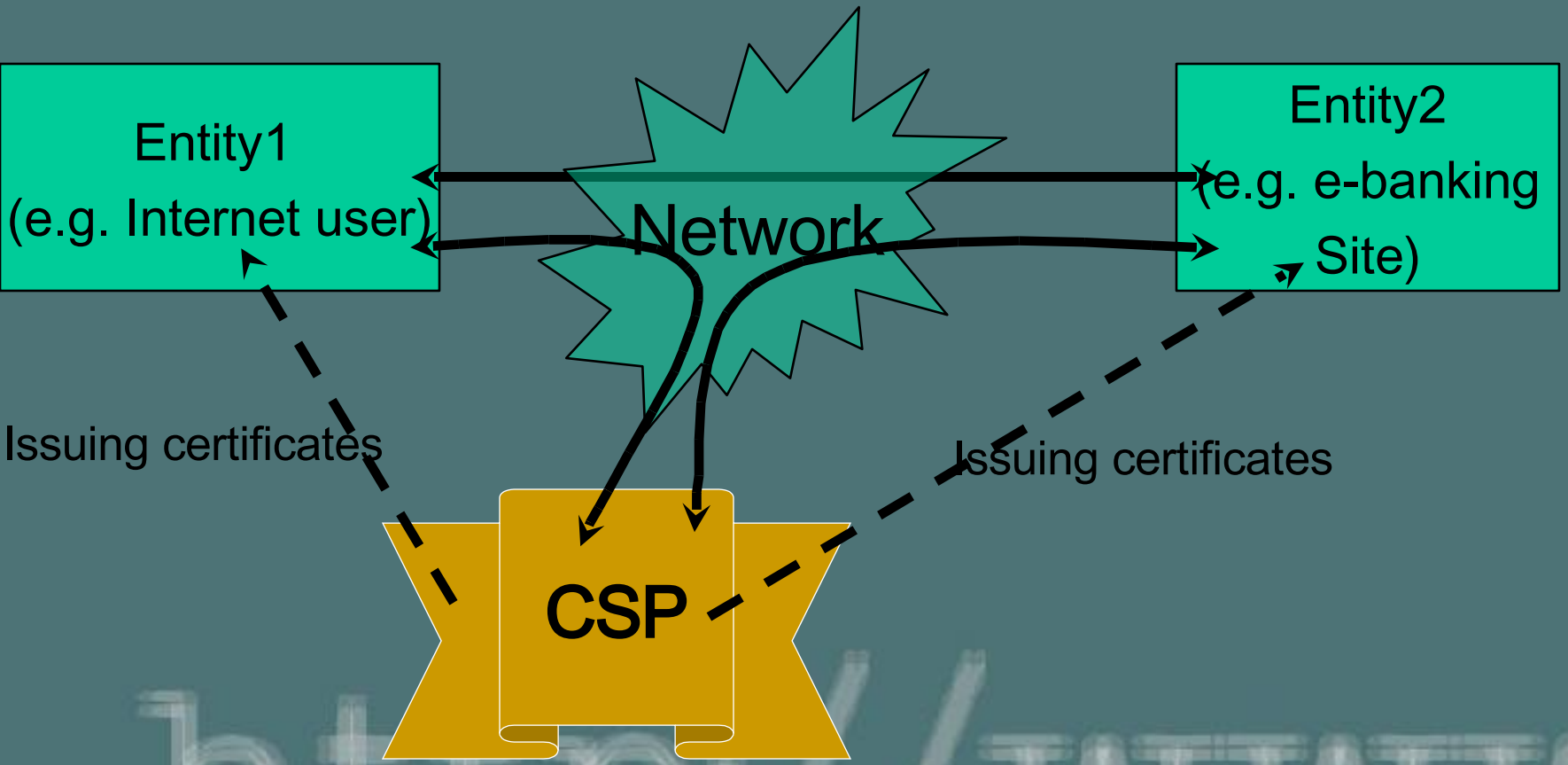
- *monitoring of communication lines*
  Encryption with randomly generated shared session key
- *shared session key stealing/guessing*
  -cryptographically secure random key generators
  -encryption of shared session key with the public key of the receiving entity
- *Non-authorised modification of (in-transit) information*
  secure hashing algorithms for message authentication codes

Facing Threats (cont.)

- *Masquerade - Web spoofing*
  Exchange of X509v3 certificates and verification against a Directory
- *Password stealing*
  Passwords are never transmitted in the network
- *Unauthorised access*
  Local Access Control List. Authentication using certificates



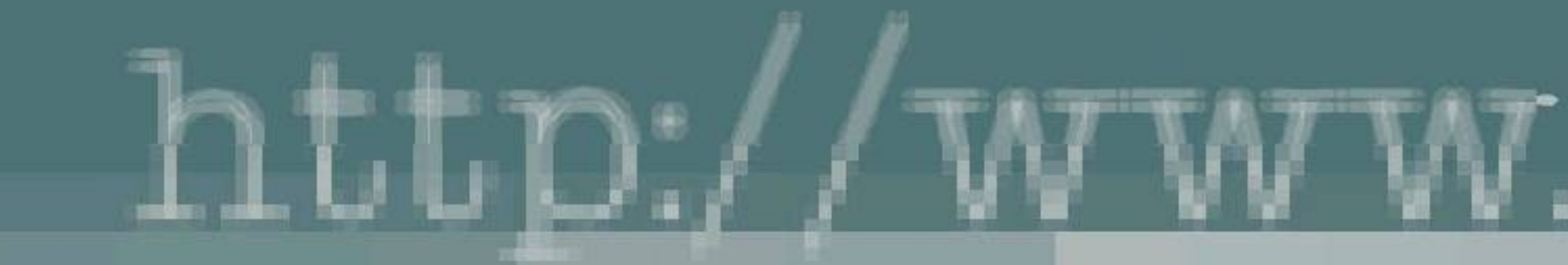
Securing electronic transactions using Public Key Infrastructure



Certification Service Provider : The Cornerstone of Public Key Infrastructure

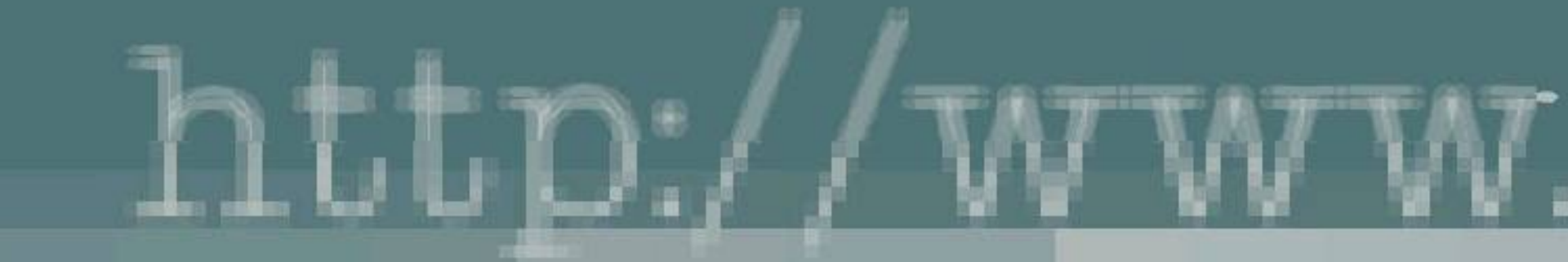
TTP : "an impartial organisation delivering business confidence, through commercial and technical security features, to an electronic transaction"

CSPs are *Trusted Third Parties* that control the life cycle of certificates



Fashion and PKI: Current trends…

- It's fashionable
- It's easy to deploy…
- It meets several security requirements, through a wide set of security services ranging from confidentiality to public notary
- It's a panacea!



Fashion and PKI: Current trends (cont.)

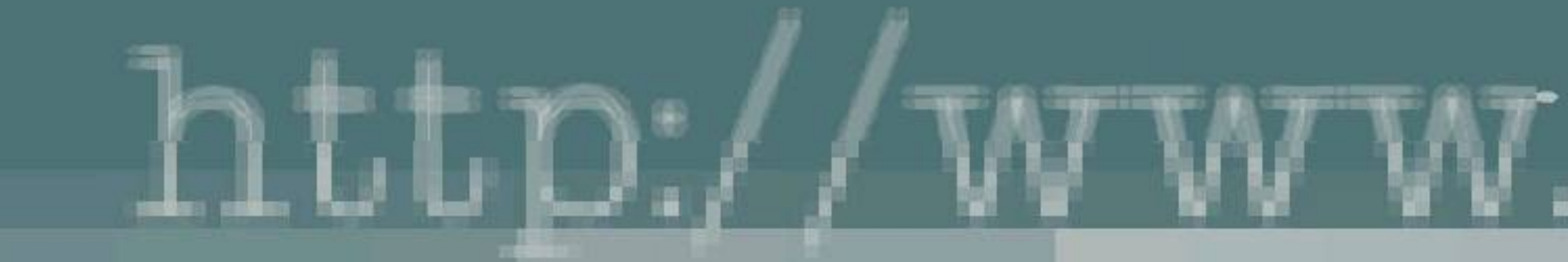
…however:

- Typical installations and operation of CSP software, withour prior analysis of requirements and without designing a Security Policy and a Certificate Policy, are a *present tense situation*, at least on an internal company-wide level. The resulting problems will soon be present and tense. PKI is nor a cure-all, neither a magical solution to security problems

Malicious Software

…*the software that contains the necessary instructions to carry out an attack to a computer system*

…*attack:* the violation (or attempt to violate) the confidentiality, integrity or availability of a system



Species of Malicious Software

Viral software

- Boot sector viruses
- Parasitic Viruses
- Multipartite Viruses
- Resident Viruses
- Stealth Viruses
- Encrypted Viruses
- Polymorphic Viruses
- Retro-Viruses
- Overwritters
- Macro Viruses

Non-viral software

- **Trapdoors**
- **Logic Bombs**
- **Trojan Horses**
- **Worms**
- **Bacteria**
- **Hoaxes**

Confronting with Malicious Software

- Security Awareness
- Antivirus Software
- Operating System logs
- Strict access control
- Forbid the execution of mobile code/programs downloaded from the Internet
- Firewalls
- Intrusion Detection Tools
- Documented procedure for recovery from Malicious Software infection
- Co-operation with the organisations that produce antivirus products

Confronting with Attempts to Intrude

Intrusion Detection Systems

- ***Anomaly Detection***

  They detect a series of actions that are unusual to occur, at least in that sequence

- ***Misuse Models***

  They detect a series of actions that are known to violate the security policy

- ***Specification based***

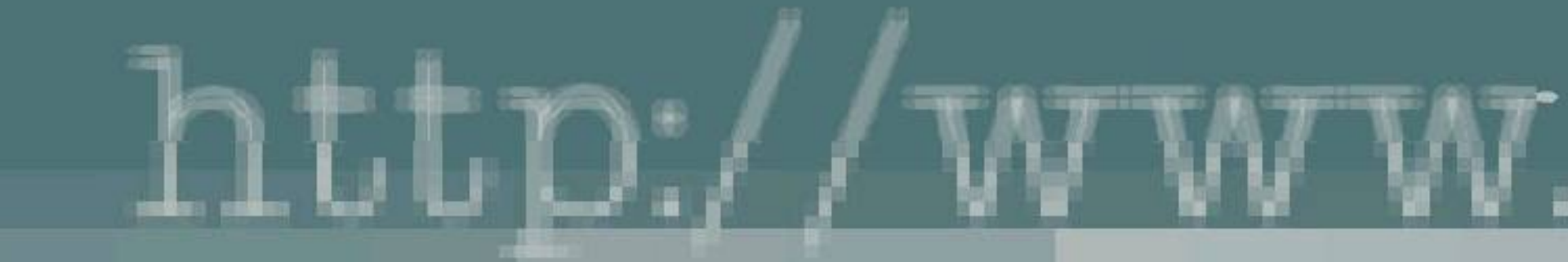
  They detect a series of actions that do not comply with the specifications the IDS has been made aware of

E-commerce and Legal Issues

- Basic liability for online activities (Computer Misuse Act, UK)
- Legal restrictions on the movement and use of cryptographic technology (USA)
- Digital signature and electronic signature laws
- Electronic `money'
- Corporate re-organisation and the IT security manager (Data Protection Act)
- Regulation of CAs/TTPs
- Data privacy legislation
- Taxation of e-commerce

Social Engineering

… the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker



Securing E-Commerce: Summary

Network Security

- Firewalls
- Packet—filtering routers
- Application-level proxy
- VPNs
- Intrusion Detection Systems (IDS)
- Network-based IDS

Securing E-Commerce: Summary (2)

Application Security

- Secure Electronic Payments
  - Secure Electronic Transactions (SET), Secure Socket Layer (SSL)
  - Electronic cash
  - Micropayments
- Chipcard protection, electronic wallets
- Content protection (digital watermarking)

Other

- **Biometric technology**
- **Public Key Infrastructure**
- **Other privacy issues (remailers, rewebbers PyTHIA)**
- **Antivirus Software**
- **Legal protection (Data Protection, Digital Signature, Computer Misuse Act)**
- ***Security awareness!***

E-Commerce Security Survey on Greek SMEs (1)

- Questioned whether there has been a security violation in their network:
  - 62% answered no
  - 21% answered yes
  - 16% answered “Don’t answer”
- Protection measures based on
  - Internal knowhow (76%)
  - External consultants (24%)
- less than 50% of authorities have elaborated plans for the continuation of their business activities

Source: E-business forum, Work cycle B, Task Force TF B1, “Information & Communication Systems Security in e-Business”

E-Commerce Security Survey on Greek SMEs (2)

- 47% of authorities have contacted the Personal Data Protection Agency within the framework of business activities
- 45% of businesses stated that their website/ webpage contains a privacy statement
- almost all businesses stated that they believe that fears and hesitations on the protection of personal data have dissuaded consumers from making internet transactions.

Source: E-business forum, Work cycle B, Task Force TF B1, “Information & Communication Systems Security in e-Business”

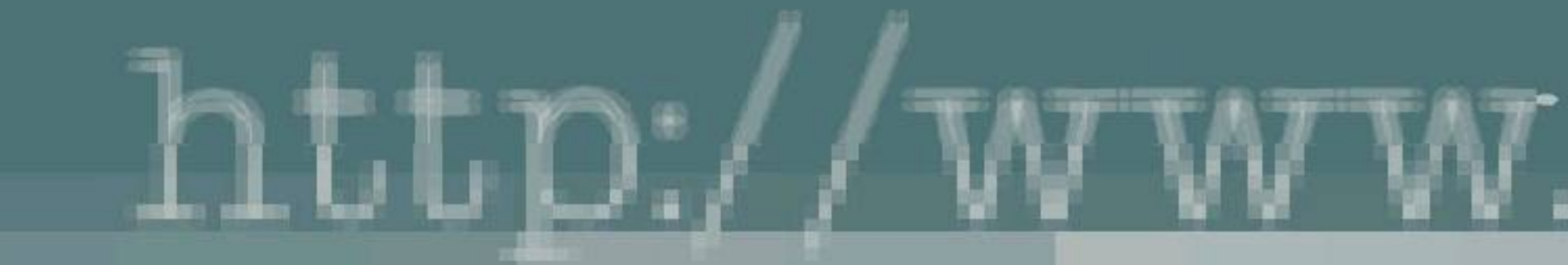
A Survey of E-Payment and M-Payment Systems

Secure Electronic Transaction Protocols

- Visa 3-D Secure international.visa.com/fb/paytech/secure/
- Bank Internet Payment System (BIPS, www.fstc.com)
- Fix (www.fixprotocol.org)
- Homebanking Computer Interface (HBCI, www.hbci.de)
- Open Financial Exchange (www.ofx.net/ofx/default.asp)
- Secure Electronic Transaction (SET, 56www.setco.org)
- Universal Cardholder Authentication Field (UCAF, http://www.mastercardintl.com/newtechnology/ecommercesecurity/spa/ucaf.html)
- Jalda (www.jalda.com)
- Magic Axess (www.magicaxess.com)

Secure Electronic Transaction Protocols (2)

- XMLPay (www.verisign.com/developer/xml/xmlpay.html)
- OBI (Opening Buying on the Internet, www.openbuy.org)
- IOTP (Internet Open Trading Protocol, www.iotp.org/)
- Echeck (www.echeck.org)

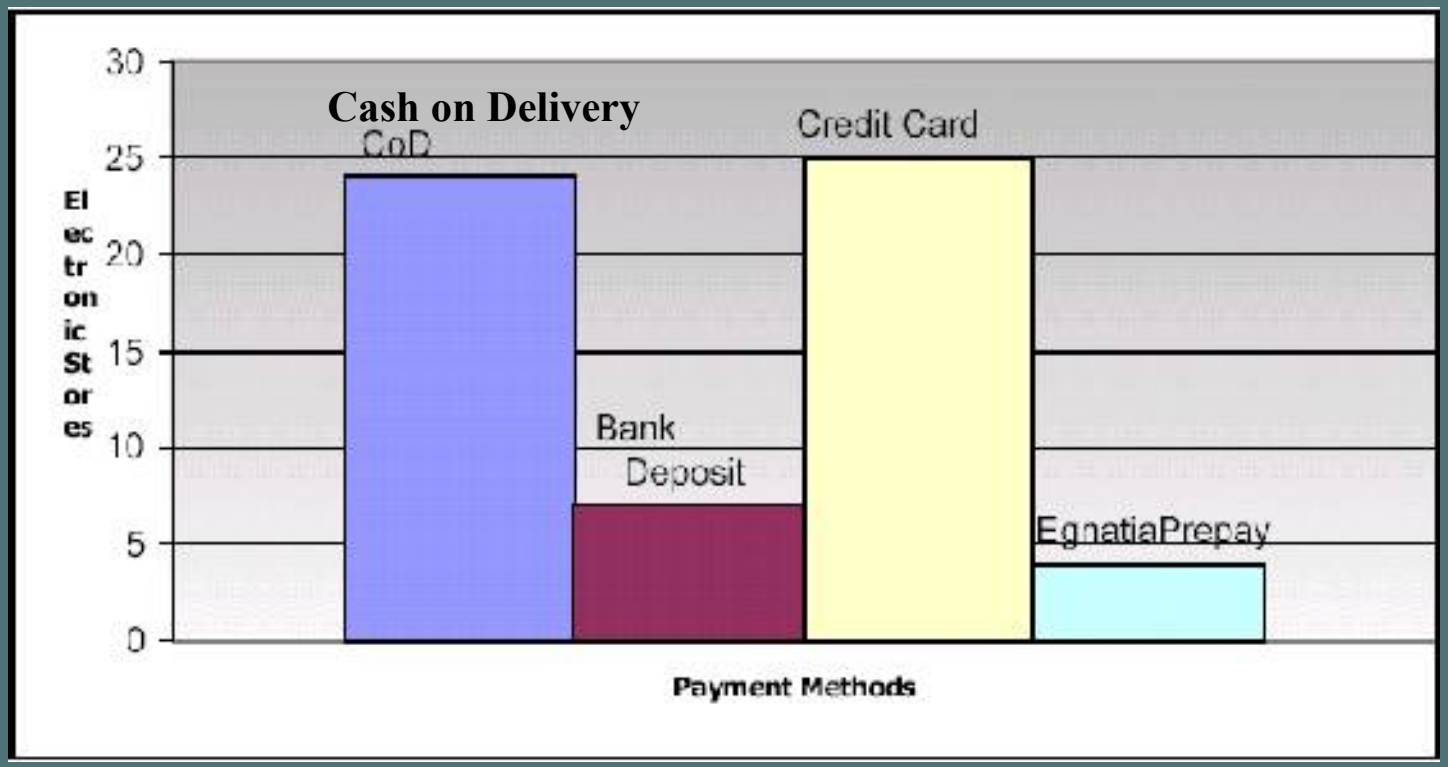


E-payments: a definition

"… the term electronic payments includes any payment to businesses, banks or public services from citizens or businesses, which are executed through a telecommunications or electronic network using modern technology"

Source : e-Business Forum, E´ Work Cycle: Work Group E3, Summary of Final Results on Electronic Payment: Problems and Perspectives

E-payments in Greece: a survey



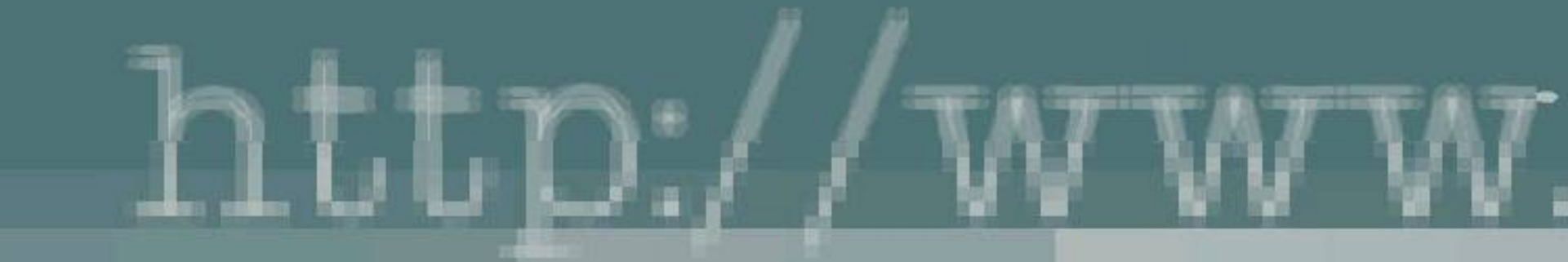
The results in the chart above stem from a study of the Work Group E3, of e-Business forum. The sample data was 30 electronic stores, selling a variety of goods.

E-payment systems

- E-cash payment systems
- Micropayment systems
- Mobile payment systems

E-payment Systems: E-cash payment systems

- Ecash (www.digicash.com)
- CAFÉ (www.semper.org/sirene/projects/cafe/)
- NetCash (www.isi.edu/gost/gost-group/)
- Mondex (www.mondex.com)
- AMADIGI (www.oakington.com/amadigi.htm)
- SmartAxis (www.smartaxis.com)
- Bibit (www.bibit.com)
- CyberCash (www.cybercash.com)



Micropayment Systems

- Millicent (www.millicent.com)
- PayWord (theory.lcs.mit.edu/~cis/pubs/rivest/RivestShamir-mpay.ps)
- MicroMint (theory.lcs.mit.edu/~cis/pubs/rivest/RivestShamir-mpay.ps)
- CEPS (www.ecbs.org)
- CLIP (www.europay.com)
- Visa Cash (international.visa.com/ps/products/vcash/)
- VISA Direct (www.visa.de/presse/presse_15112002.htm)
- Yahoo PayDirect (paydirect.yahoo.com)

MicroPayment Systems (2)

- iPIN (www.ipin.com)
- W-HA (www.w-ha.com)
- WISP (www.trivnet.com)
- Telia PayIT (www.telia.se)
- AvA (www.leskiosques.com/V2/k_webwap/ava/index.htm)
- Cartio MicroPayments (www.cartio.com)
- InternetCash (www.internetcash.com)
- Coulomb IMPS (www.coulomb.co.uk)
- Geldkarte (www.scard.de)
- Proton (www.protonworld.com)

Mobile payment systems

- TELEPAY (www.ertico.com/activiti/projects/telepay/home.htm)
- Sm-PaySoc (www.smpaysoc.org)
- Sonera (www.sonera.fi/english/)
- PayBox (www.paybox.net)
- PayByTel (www.paybytel.net)
- M-pay bill (http://mpay-bill.vodafone.co.uk)
- Mobipay (www.mobipay.com)
- Visa Movíl (www.visa.es)
- Street Cash (www.streetcash.de)

Mobile payment systems (2)

- Safetrader (www.ehpt.com)
- EartPort (www.earthport.com)
- SPA - Secure Payment Application (http://www.mastercardintl.com/spa/)
- EMPS (http://www.nordea.fi/E/Merita/sijoita/uutta/990524.ASP)
- GiSMo (www.gismo.net)
- Fundamo (www.fundamo.com)
- Faircash (www.e-faircash.com)
- eCharge Phone (www.echarge.com)
- Genion m-payment (www.genion.de)

Mobile payment systems (3)

- Easybuy (http://www.gsmagazine.com/timeasybuy.htm)
- NewGenPay (www.newgenpay.com)
- eTopup.com (www.etopup.com)
- MoxMo (www.moxmo.com)
- Beam Trust (www.beamtrust.com)
- i-mode (www.nttdocomo.co.jp/english/p_s/imode/index.html)

Case Study: ATM Fraud

Case Study: Automatic Teller Machines

Security awareness is of paramount importance; the best security countermeasures can become useless due to the human factor

Social Engineering

- Sign posted at an ATM (Maryville, Tennessee, USA) reading
  "Due to recent fraud attempts at this ATM machine, we require you to swipe your card in the reader below before using the machine“,
- Enquiries over the phone, regarding personal data of the subject, on behalf of the bank and for verification purposes,

Case Study: Automatic Teller Machines (2)

- Card retained in ATM (plastic flap was glued over the slot, blocking the card from exiting). As the customer struggles to get the card, a passer-by approaches, offers help and asks the customer his PIN number. After faking an effort to remove the card, the passer-by leaves, and when the customer leaves the area too, the malevolent passer-by returns to collect the card,
- shoulder surfing,
- card traps (skimming),
- physical violence.

Q&A