A journey in the world of PKI

PKI: *Overpromising and underdelivering*

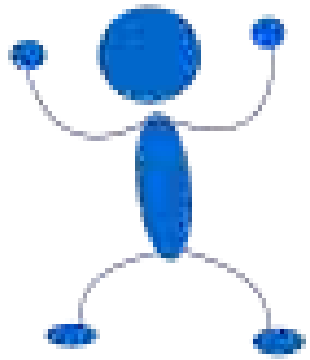
Still a long way to go...

John Iliadis, jiliadATpanafonet.gr
TEIRESIAS Banking Information Systems
&
De Facto Joint Research Group on
Information and Communication Systems Security
University of the Aegean

Contents

- Prologue
- Quick Overview
- Security
- Cryptography
- PKI
- PKI Outside Wonderland and into the Real World
- Summing it up

PKI! Great security solution!

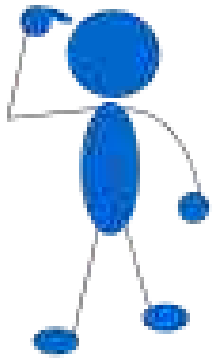


- Let's do it!

PKI Implementation

Prologue, Part 3

Now, let me see....



- ...what were the problems we wanted PKI to solve?
- ...and what about the problems introduced by PKI?

Quick Overview

- Information Security: back to the basics
- What makes (or makes not) asymmetric crypto so special?
- Digital Signatures
  - Technical Framework
  - Legal Framework

  ...then how come they are still not there?
- PKI (outside Wonderland)

Section 1: Information Security

- What isn't Information Security?
- What is Information Security?
- What is Risk Analysis?
- What is Security Policy?
- Information Security Lifecycle
- Approaches to Information Security

InfoSec != Secret Crypto Algorithms

- The *crypto algorithm* secrecy issue, by example
  1. Algorithm known only to the 2 communicating entities
     - Alice and Bob use a secret algorithm they developed to exchange confidential information.
  2. Algorithm known only to a few communicating entities
     - Telecom operator uses in-house developed secret algorithm, to encrypt intra-company wireless traffic of its clients .
  3. Different crypto algorithm for each communicating pair
     - Telecom operator uses a different in-house developed secret algorithm to encrypt the traffic of each of his clients

Which one is the more secure? Why ?

InfoSec != Secret Crypto Algorithms

- Super-secure secret algorithm #1
  - Ciphertext = “DLROWOLLEH”
  - Plaintext = ? Decryption time = ?
- Super-secure secret algorithm #2
  - Ciphertext = “LHOORZRUOG”
  - Plaintext = ? Decryption time = ?
- Super-secure secret algorithm #3
  - Ciphertext = “HELLOWORLD”
  - Plaintext = ? Decryption time = ?

InfoSec != Secret Crypto Algorithms

- Quality of secret encryption algorithms
  - Range from “Potentially very good” to “No encryption used whatsoever” (e.g. XOR)
- Cryptanalysis attempts
  - The more people try to “break” (find deficiencies in the design of) a crypto algorithm, the sooner they may reach their goal
- Good encryption algorithms can only be public
  - They are meant to be public, so they can be reviewed and amended by as many cryptographers as possible.
- What about DES, SHA-0?

InfoSec != Obscurity

- Internet
  - *Obscurity:* Running a Web Server at port 37649, so that only your associates, whom you 've told the port number, can connect to it
  - *No security:* A port scan would reveal the port in seconds
- Software
  - *Obscurity:* Keeping secret an exploitable vulnerability you discovered in your software
  - *No security:* Once the bad guys find out about it, the good guys will be unprotected, running unpatched and vulnerable software

Security is about… (1)

- "The only good locks are open, public and accessible ones", W. Diffie
  - Can be studied by many people at the same time
  - Vulnerabilities discovered and disclosed
  - Corrective actions or patches researched and disclosed

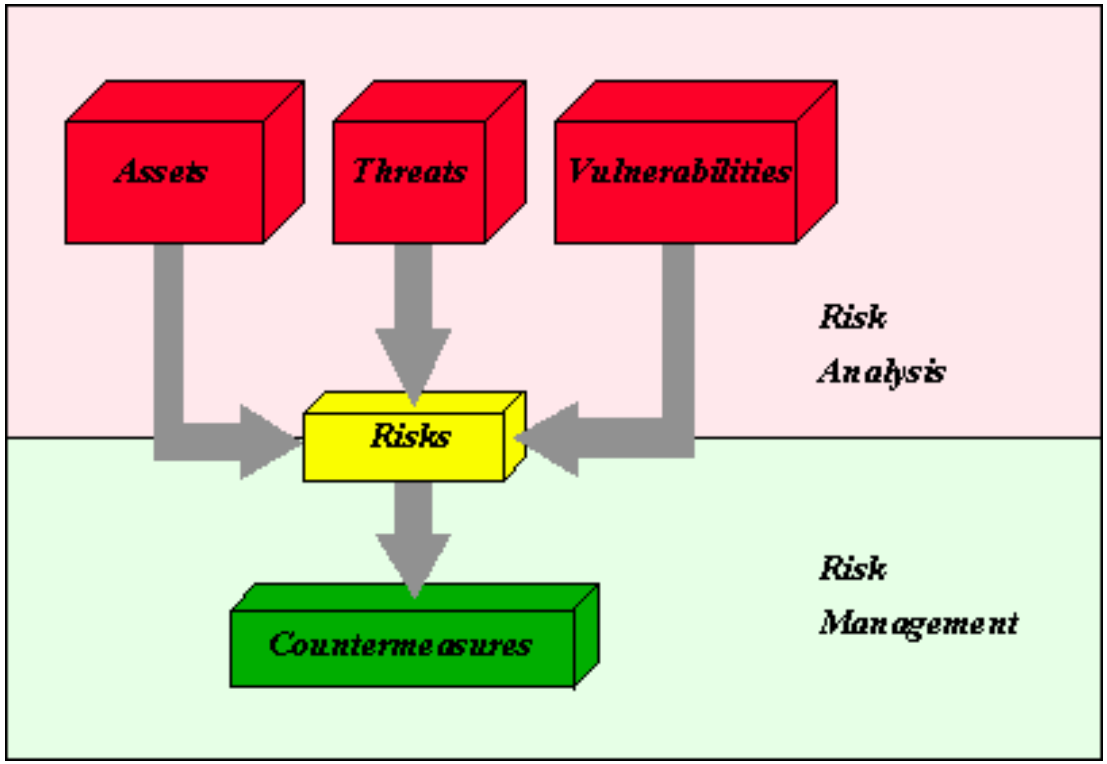
- Security is an enabler for business
  - It enables businesses to do things they couldn't do before, because they were too risky

Security is about... (2)

- How many kilograms of Security would you like?
  - Organisations' cost for implementing countermeasure <= organisations' cost of suffering breach
  - Hacker's cost for breaching security >= hacker's profit of breaching security
    - *Threat*: Blank 3.5" disks disappear from your office, every once in a while...
    - Countermeasure: Buy a safe and store your blank 3.5" disks there
- Security does not solve problems, it changes the problem's domain, e.g.
  - Confidentiality of information -> Confidentiality of key

Security is about... (3)

- Risk Analysis
  - What is at risk (assets)
    - Qualitative analysis
    - Quantitative analysis
  - What vulnerabilities can be exploited
    - Technical
    - Process
    - People
  - What threats exist
  - Risk management
    - Eliminate/reduce risk
    - Accept risk
    - Transfer risk



CRAMM-based Risk Analysis

Security is about... (4)

- CIA
  - Confidentiality
  - Integrity
  - Availability
- More Information Security objectives
  - Entity authentication
  - Data authentication
  - Non-repudiation

Security is about... (5)

- Information Security Policy
  - The basis for all information security efforts
  - Directs how issues should be addressed and technologies should be 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

Security is about... (6)

- Information Security Lifecycle
  - Risk analysis
  - Security policy
  - Overall system re-engineering (even better: security built-in, from the start)
  - Security management of deployed system
  - Incident Response
  - Business Continuity Planning

Bottom-Up Approach to Security

- System administrators trying 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

Section 2: Cryptography

- Symmetric & asymmetric crypto: A simplified scenario
- Key Distribution
  - Symmetric cryptography
  - Asymmetric cryptography
- Differences between symmetric and asymmetric
- Typical algorithms used in PKI
- Applications of cryptography

Symmetric & asymmetric cryptography:

A simplified scenario

A simple scenario: Symmetric Crypto (1)

Alice

Document

Symmetric key
“pass21”

Encrypt

Bob

Symmetric key
“pass21”

Encrypted
document

Decrypt

Document

A simple scenario: Symmetric Crypto (2)

- Both Alice and Bob must have the same key (“pass21”)
- Encryption/decryption:
  - Step 1: Alice encrypts the document with key “pass21” and sends to Bob the encrypted document
  - Step2: Bob receives 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. ensure the *key's confidentiality.*

A simple scenario: Asymmetric Crypto (1)

Alice

Bob's public key
"dfgsd34"

Document

Encrypt

Bob

Bob's private key
"3trer4"

Encrypted
document

Decrypt

Document

A simple scenario: Asymmetric Crypto (2)

- Bob has a keypair (a public key and a private key)
- Encryption/decryption:
  - Step 1: Alice encrypts the document with Bob's public key "dfgsd34" and sends to Bob the encrypted document
  - Step2: Bob receives 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. ensure *the integrity of his public key*.

- Basic services of Key Management (ISO 11770)
- Key Distribution in symmetric cryptosystems
- Key Distribution in asymmetric cryptosystems

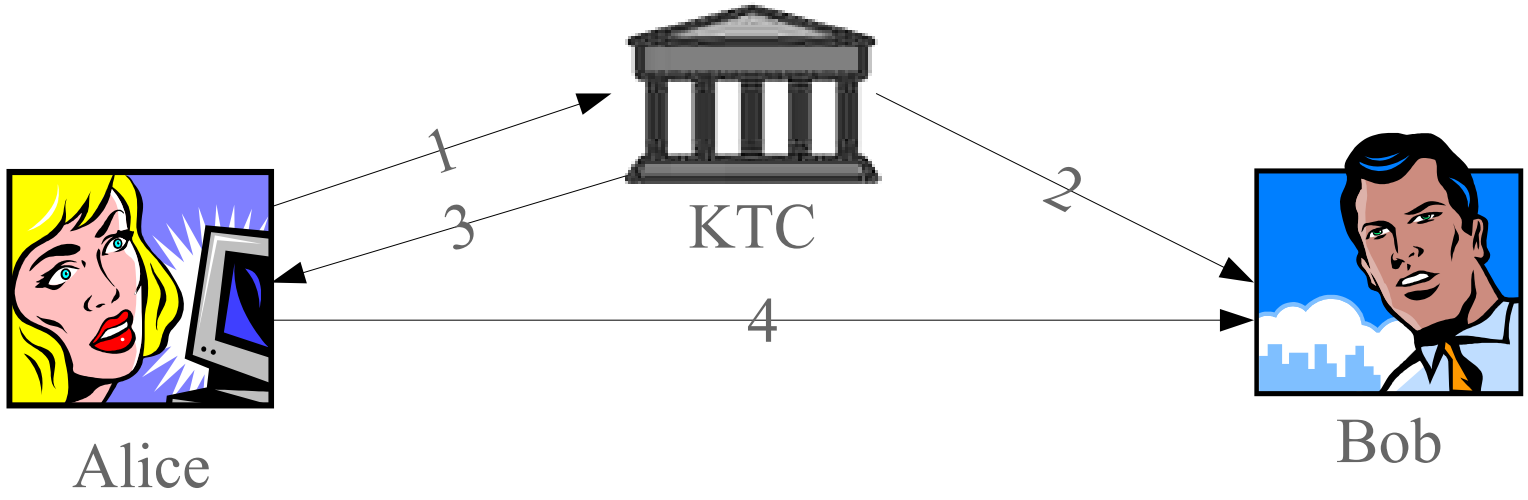
Basic services of Key Management

- Generate-Key
- Register-Key
- Create-Key-Certificate
- Distribute-Key
- Install-Key
- Store-Key
- Derive-Key
- Archive-Key
- Revoke-Key
- Deregister-Key
- Destroy-Key

Key Distribution in Symmetric Crypto

- Direct
- Key Translation Center
- Key Distribution Center
- more...

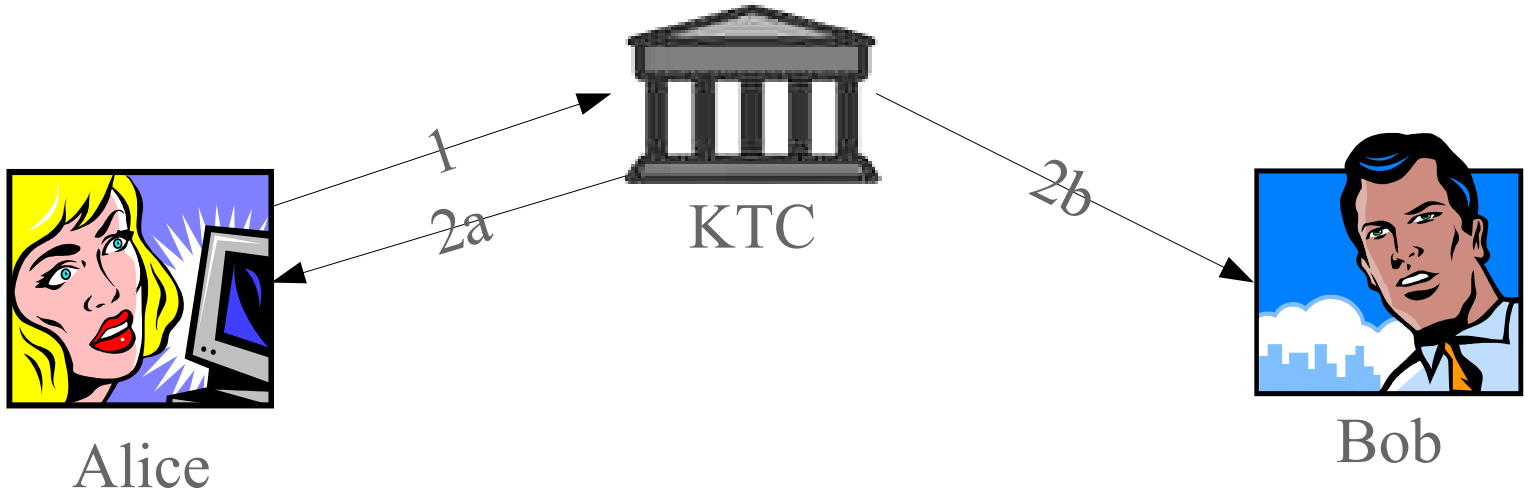
Key Translation Center



Translation Methods
- Steps 1,2, OR
- Steps 1,3,4

1. Alice->KTC: Enciphered key
2. KTC->Bob: Re-enciphered key, OR
3. KTC->Alice: Re-enciphered key AND
4. Alice->Bob: Re-enciphered key

Key Distribution Center



1. Alice->KDC: Request for shared key

2a. KDC->Alice: Enciphered shared key

2b. KDC->Bob: Enciphered shared key

If KDC cannot communicate securely with Bob (2b), then Alice assumes responsibility for distribution of enciphered shared key to Bob

Key Distribution in Symmetric Crypto - A Note

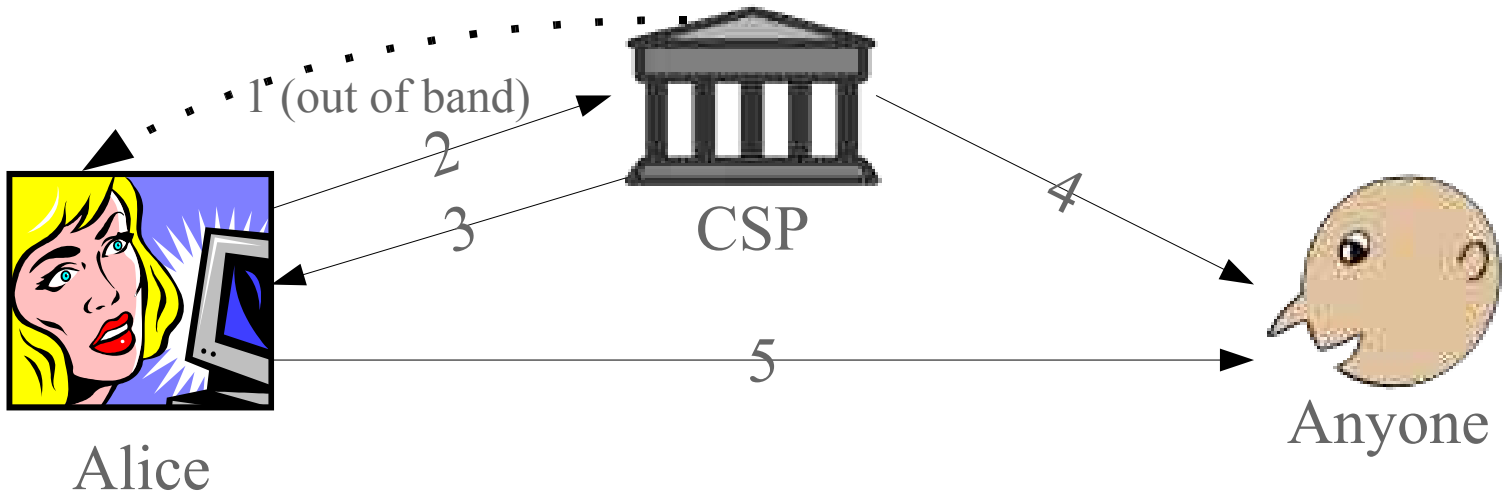
- All mechanisms (except the *Direct* one) require

1. Shared symmetric or asymmetric key
2. Inline Key Center

Key Distribution in Asymmetric Crypto

- Protected channels
  - Data origin authentication
  - Data integrity protection (e.g. courier and registered mail)
- TTP-assisted (i.e. certificates)

Certificate Service Provider



Distribution Methods
- Steps 1,2,3,4 OR
- Steps 1,2,3,5

1. Alice receives CSP public key (out of band)
2. Alice->CSP: Key_{Alice}
3. CSP->Alice: $Certificate_{Alice}$
4. CSP->Bob: $Certificate_{Alice}$ OR
5. Alice->Bob: $Certificate_{Alice}$ (by itself or in S/MIME)

Key Distribution in Asymmetric Crypto - A Note

- Key Distribution requires
  - Integrity protected channel, or
  - An offline TTP
- Other TTP operational requirements, like revocation, necessitate online operation of TTPs

Symmetric/Asymmetric Crypto: Differences

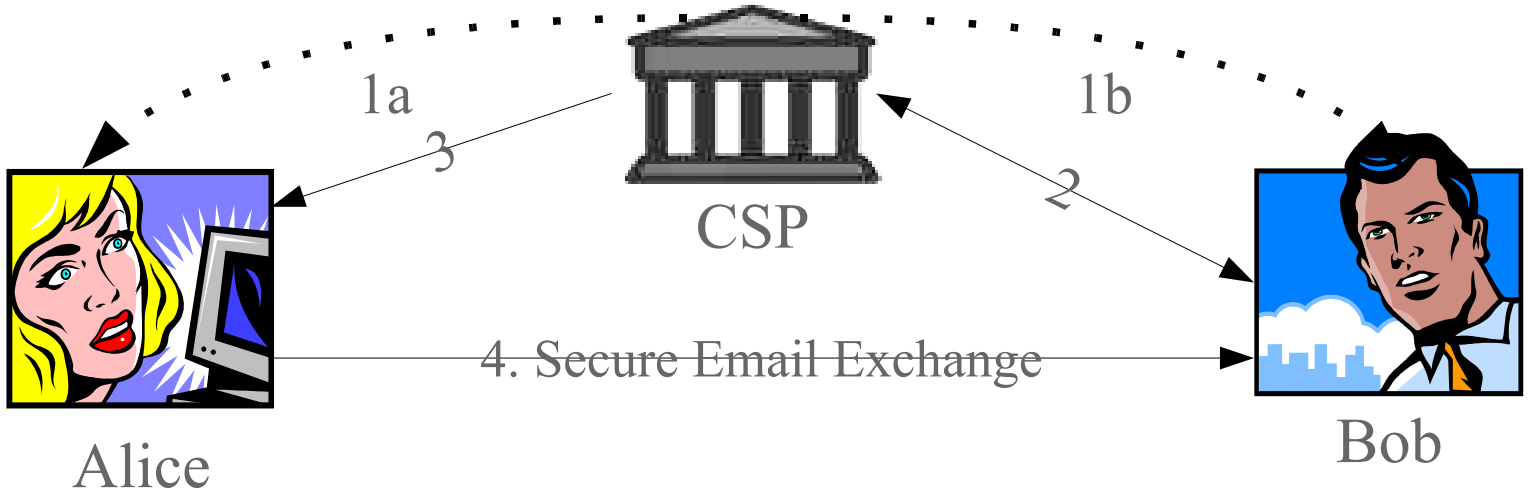
- Symmetric cryptosystems
  - Use of one key, shared between A(lice) and B(ob),
  - Ensure the *confidentiality of the shared key*
- Asymmetric cryptosystems
  - Use of a keypair (public+private) for each communicating party
  - Ensure the *integrity of the public keys*

Typical algorithms used in PKI

- Symmetric ciphers
  - DES, 3-DES, AES, RC4
- Hash functions
  - MD5 (vulnerable) , SHA-1, RIPEMD (RSA 2004-2005 conferences, collisions)
- Asymmetric ciphers
  - RSA, DSS, El-Gamal

- Applications of Cryptography
  - Exhanging secure e-mails (e.g. S/MIME, PGP)
  - Secure access to Web resources (e.g. HTTP over SSL)

Exchanging Secure E-mails (1)

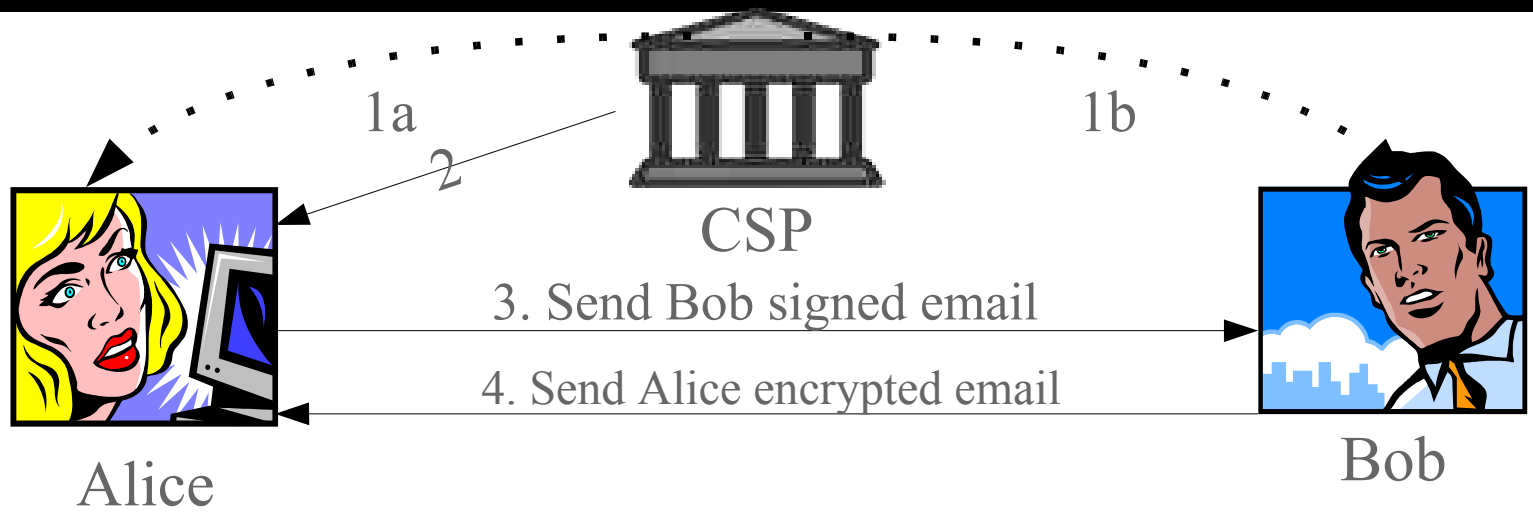


1. Steps 1a,1b : Out of band transport of CSP certificate
2. Step 2 : Certificate request and distribution
3. Step 3 : Download Bob's certificate
4. Step 4 : Send encrypted e-mail; enveloping

a) Alice sends $A=E_{bob's\_Cert}(random\_symmetric\_key)$, $B=E_{random\_symmetric\_key}$ (email message)

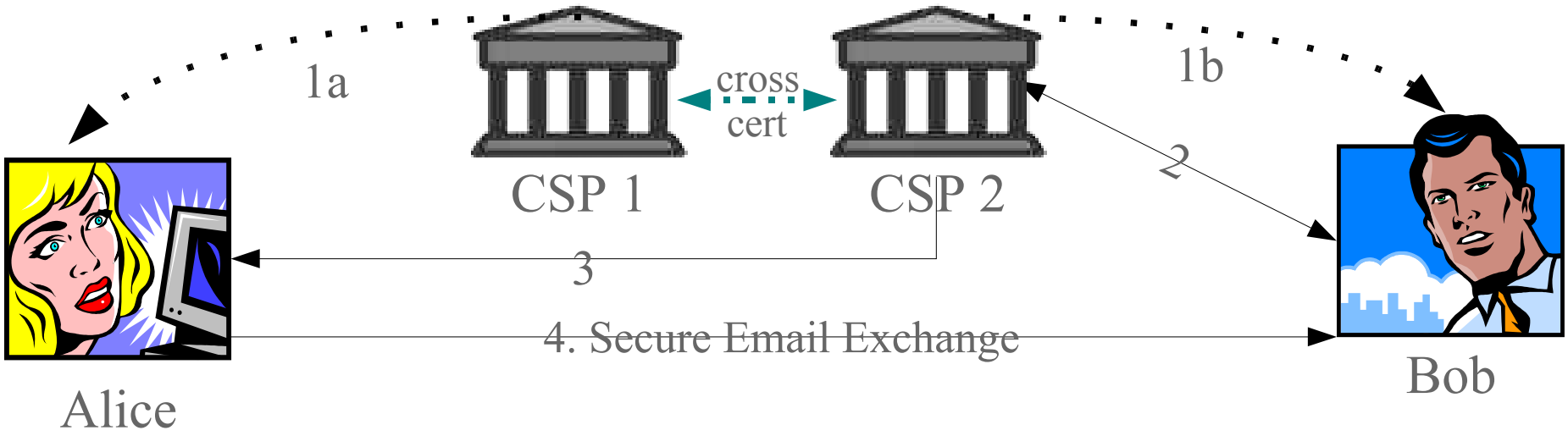
b) Bob decrypts email: $C=D_{bob's\_Private\_Key}(A)$, $D_C(B)$

Exchanging Secure E-mails (2)



1. Steps 1a,1b : Out of band transport of CSP certificate
2. Step 2 : Certificate request and distribution
3. Step 3 : Send Bob signed email
   1. Alice sends $A=E_{Alice's\_Private\_Key}(Hash(email\ message))$, b=email message
   2. Bob verifies signature: H=hash(email message), $D=D_{Alice's\_Cert}(A)$, check if H=D
4. Step 4 : Send Alice encrypted e-mail; enveloping
   a) Bob sends $A=E_{bob's\_Cert}(random\_symmetric\_key)$, $B=E_{random\_symmetric\_key}$ (email message)
   b) Alice decrypts email: $C=D_{bob's\_Private\_Key}(A)$, $D_C(B)$

Exchanging Secure E-mails (3)

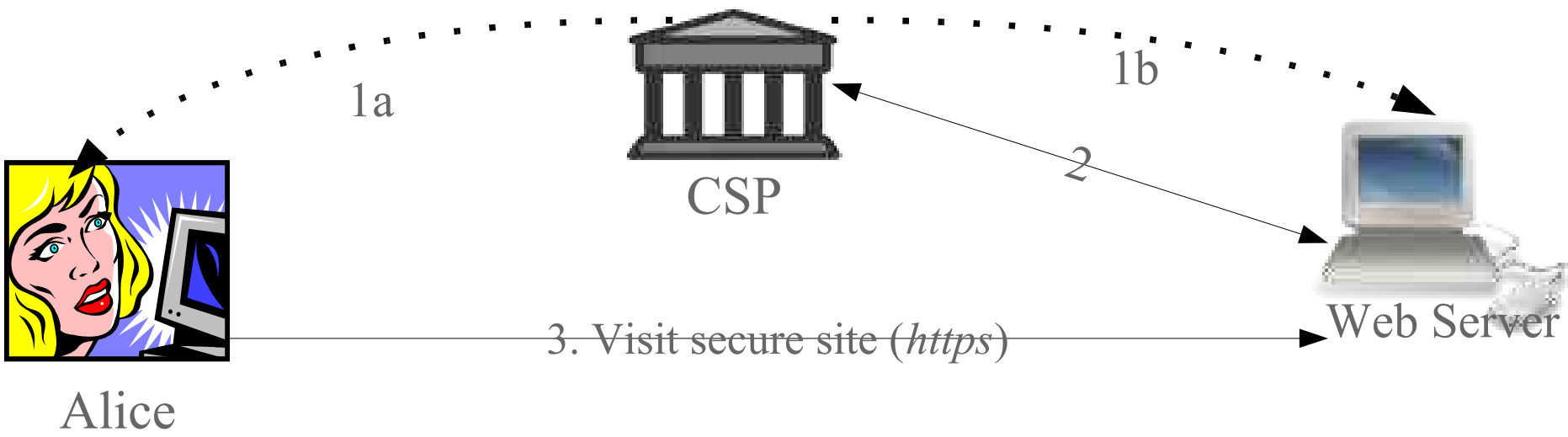


1. Steps 1a,1b : Out of band transport of CSP certificate
2. Step 2 : Certificate request and distribution
3. Step 3 : Download Bob's certificate
4. Step 4 : Send encrypted email; enveloping

a) Alice sends $A=E_{bob's\_Cert}(random\_symmetric\_key)$, $B=E_{random\_symmetric\_key}$ (email message)

b) Bob decrypts email: $C=D_{bob's\_Private\_Key}(A)$, $D_C(B)$

Secure Web Access: HTTP over SSL



1. Steps 1a,1b : Out of band transport of CSP certificate
2. Step 2 : Certificate request and distribution
3. Step 3 : Visit secure site (*https*)
   a) Alice receives Web Server's certificate (W_{cert})
   b) Alice verifies W_{cert} using the CSP certificate
   c) Alice sends $E_{WebServerCert}$(random_symmetric_key) to W
   d) Alice and the Web Server start encrypting the information they exchange, using the random symmetric key

Numbers used Once (Nonces)

- Communication can be replayed or hijacked, e.g.
  - Encrypted emails:
    - Mallory manages to cryptanalyse a specific encrypted email sent by Alice to Bob
    - Mallory produces a fake email to Bob (Alice is supposedly sending this one)
    - Mallory encrypts the email with the same symmetric key
    - Mallory attaches to the email the captured $E_{bob's\_Cert}(random\_symmetric\_key)$
  - Solutions
    - Numbers used Once
    - Timestamps (trusted time source?)

Public Key Infrastructure

Section 3: Public Key Infrastructure

- Certificates – what are they?
- Digital Signatures
  - What are they ?
  - Comparison to handwritten signatures
- Trusted Third Parties
  - Certification Service Providers
  - Trust Models
  - Certificate Status Information
- EU Directive 1999/93/EC and its implications
  - Qualified certificates and advanced electronic signatures

Certificates: What are they ?

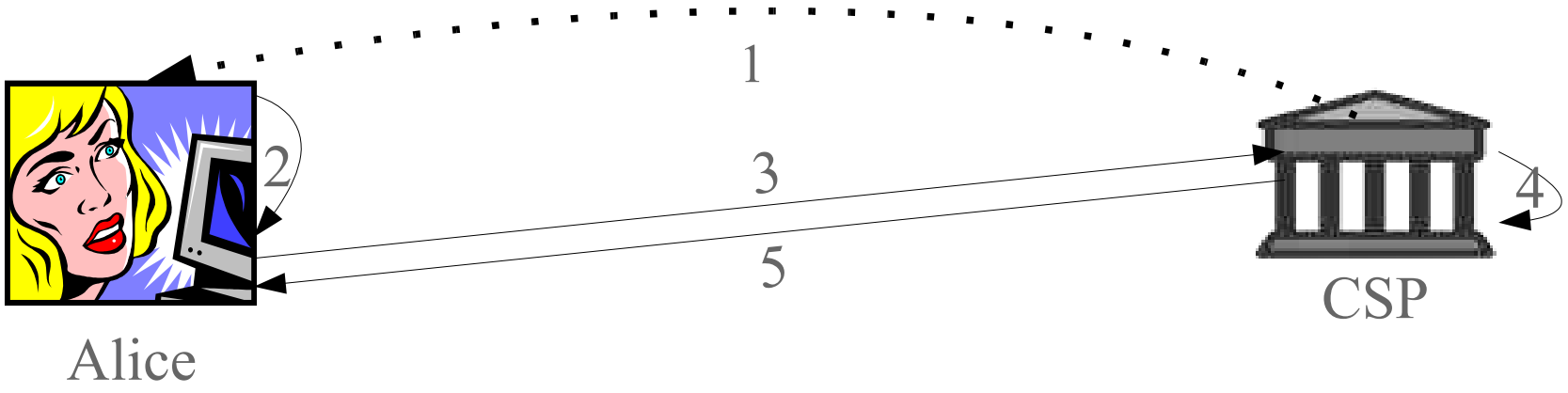
Certificates - What are they ?

- Offline authentication token
- X.509v1-3
- Proprietary extensions
- Criticality of extensions

- Identification info of holder
- Identification info of CSP
- Public key of holder
- Expiration date
- Extensions (e.g. Key Usage, CSI location)
- Digitally signed by CSP

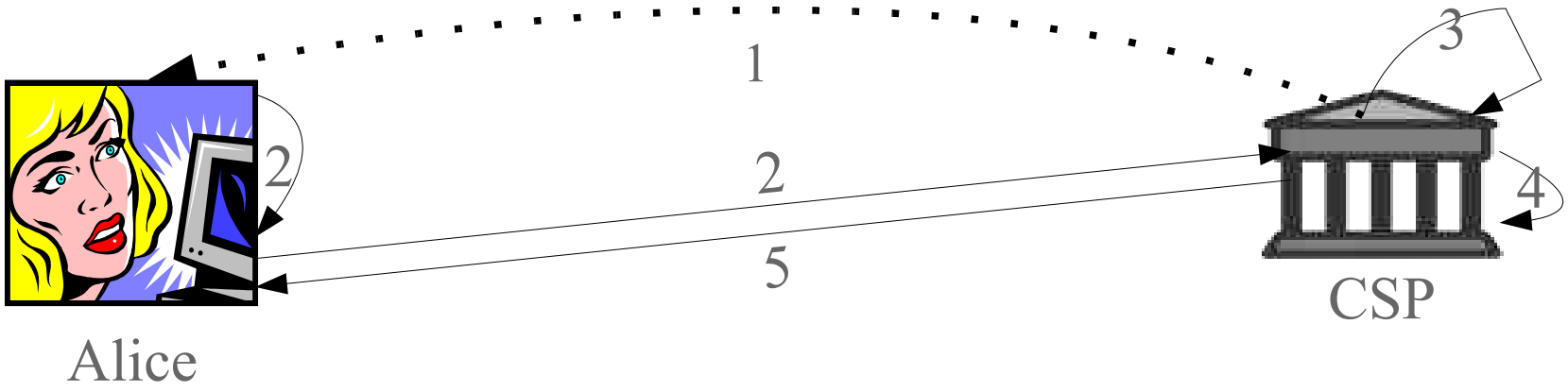
X.509v3 Certificate

Issuing Certificates (1)



1. Alice receives CSP certificate (out of band)
2. Alice produces her own keypair (public+private key)
3. Alice securely (e.g. SSL) uploads her public key to CSP, for certification
4. CSP binds Alice's public key to Alice's identification information and signs
5. CSP sends the certificate to Alice

Issuing Certificates (2)



1. Alice receives CSP certificate (out of band)
2. Alice communicates securely with CSP (e.g. SSL) and requests a certificate
3. CSP produces new keypair for Alice
4. CSP binds Alice's public key to Alice's identification information and signs
5. CSP sends the certificate and the private key to Alice

*note: CSP does not keep a record of Alices private key (?)

Main stages in certificate lifecycle

- Key Generation
- Entity Registration
- Certificate Distribution
- Certificate Archiving
- Certificate Expiration
- Certificate Revocation

Digital Signatures

Digitally Signing and Verifying

Alice

Alice's private key

Document

Signing

Bob

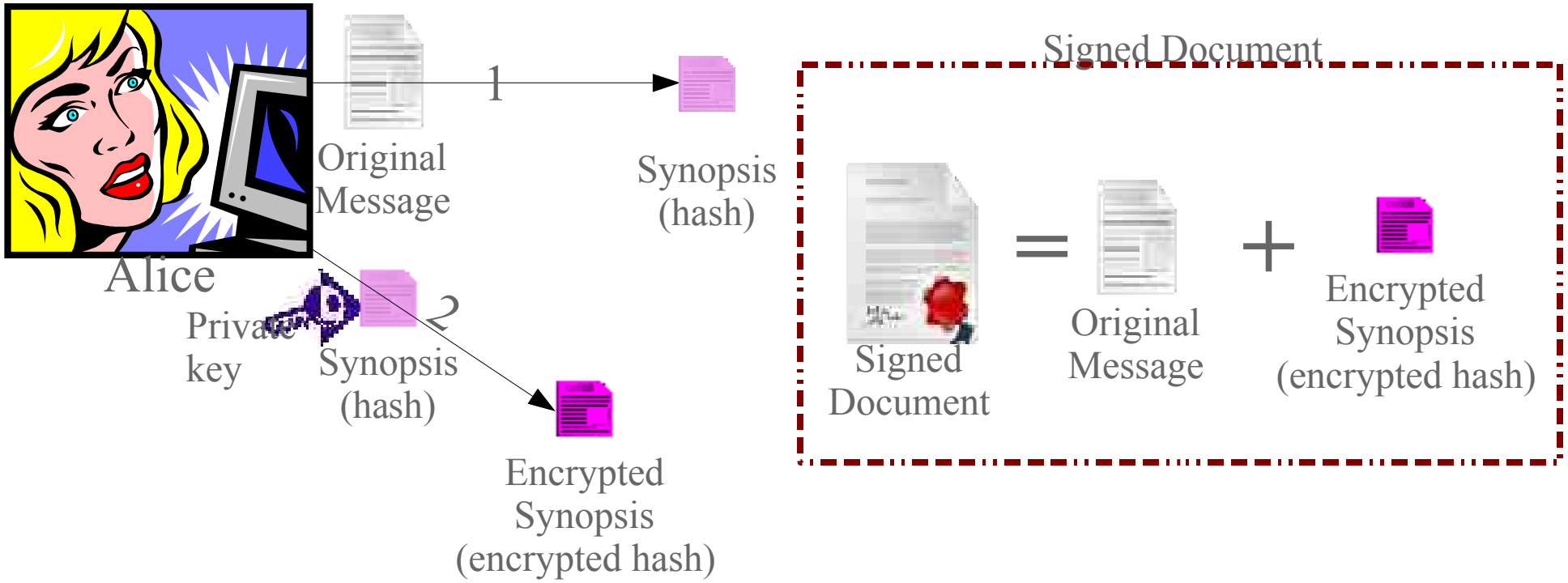
Alice's certificate

Signed Document

Verify Signature

Signed Document, Verified signature

Digitally Signing: A generic scenario



- Step 1: Produce synopsis (hash, e.g. MD5, SHA-1) of original message: H=Hash(Original_Message)
- Step 2: Encrypt H with private key: $EH=E_{Alice's\_Private\_Key}(H)$
- The signed message is composed of:
  - The original message
  - The encrypted hash (EH)

Digital Signatures: What are they ?

- Based on digital certificates
- Data authentication
- Non-repudiation
  - Timestamping
  - Non-repudiation mechanisms
  - Underlying legal framework

Signatures: Comparing digital to handwritten

	Digital	Handwritten
Data authentication	✓	✗
Data integrity	✓	✗
Non repudiation	✓ (pending other factors)	✓ (forging signatures? forging own signature?)
Does not alter the original message	✓	✗ (e.g. Legal document already signed cannot be signed by other party)

Trusted Third Parties

Trusted Third Parties

- Trusted Third Party (TTP)
  - “an impartial organisation delivering business confidence, through commercial and technical security features, to an electronic transaction”
- Certificate Service Providers (CSPs)
  - Trusted Third Parties that control the life cycle of certificates

Certification Service Providers

- Main CSP services
  - Registration
  - Key generation, personalisation, archiving
  - Certificate generation, renewal, distribution, archiving
  - Certificate revocation
  - Certificate Status Information generation, archiving (e.g. CRL)
  - Key recovery

TTP Services

- Timestamping
- Notarisation
- Data archive
- Non-repudiation
  - Online TTP
  - Inline TTP
  - Offline TTP
- ...

TTPs: Main Actors

- Certificate Authority, providing certificates.
- Registration Authority, registering users and binding their identities to certificates.
- Repositories, storage and dissemination entities containing TTP-related public material such as certificates and CRLs.
- Certificate holders, holding certificates from CAs which they use in order to sign or authenticate themselves.
- Dependent entities (US Eng.: relying parties), entities which use the certificates presented by other entities in order to authenticate the latter or verify their signature.

PKI Main Components

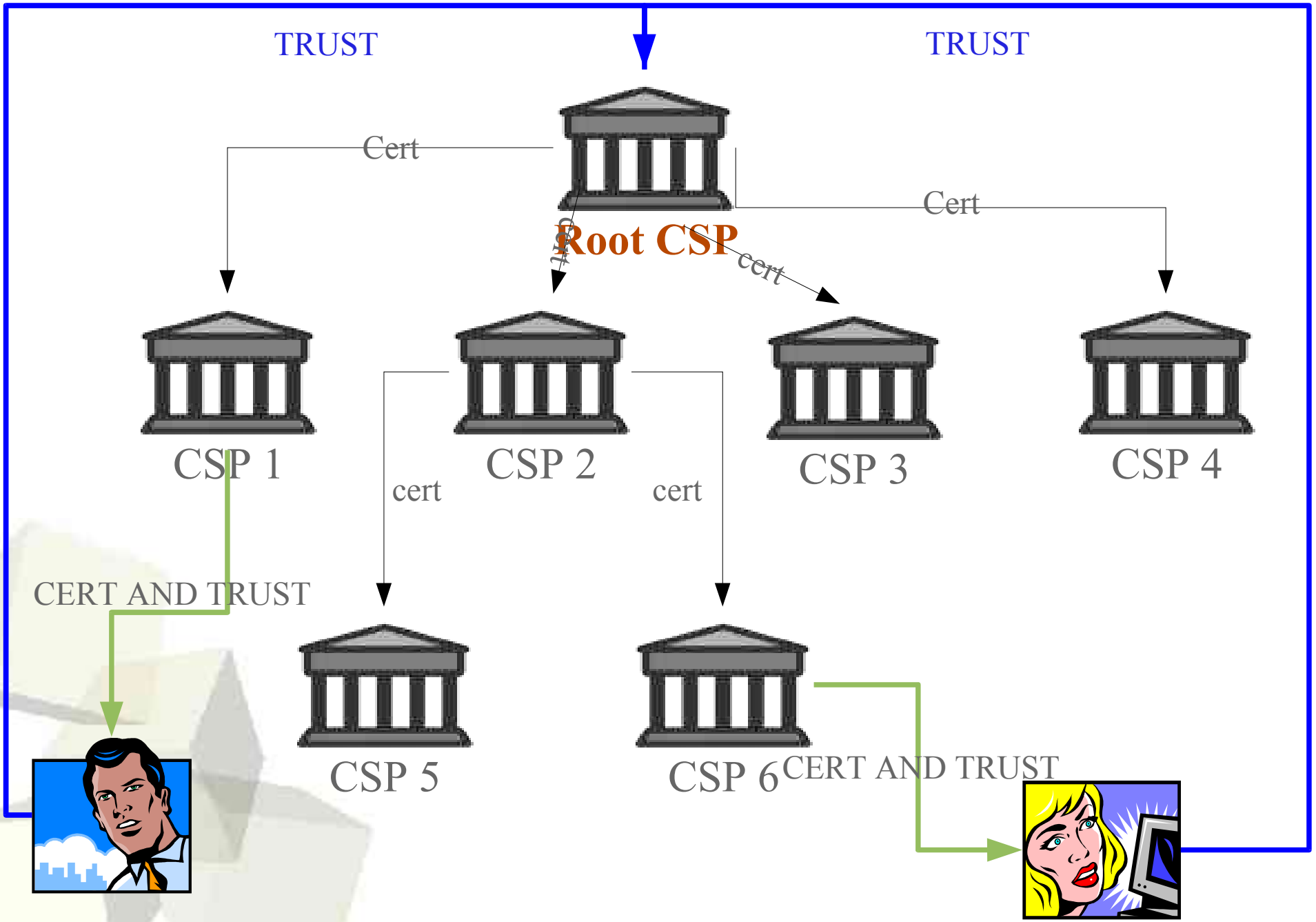
- Set of TTPs
  - Certificate Service Providers
  - Timestamping Authorities
  - ...
- Interoperability and collaboration
- Legal framework
- Value-Added services
  - Non-repudiation service
  - ...

Trust Model

- Why ?
  - Entities holding certificates from non-cooperating CSPs
  - Entities trusting only CSPs belonging in their domain (e.g. country, enterprise, etc)
  - Different trust models to accommodate for different needs

- Trust Models
  - Hierarchical
  - Flat
  - Mixed
  - Web of Trust

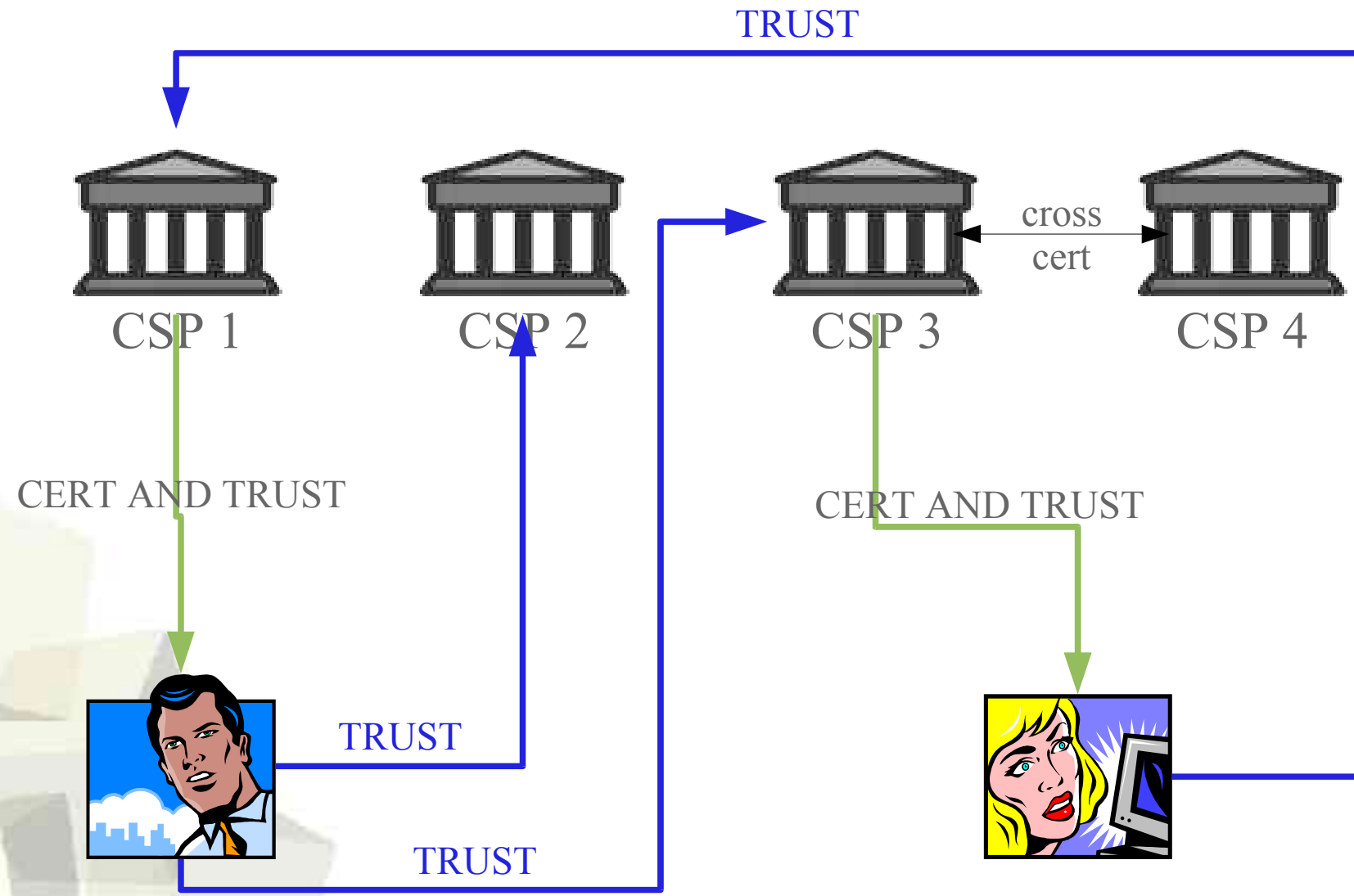
Hierarchical Trust Model (1)



Hierarchical Trust Model (2)

- Everyone has to trust the Root CA
- Quite the case in environments with strict hierarchy already defined (military, large corporations etc)
- If two entities, belonging to distant leafs, wish to communicate, they have to validate a long cert chain

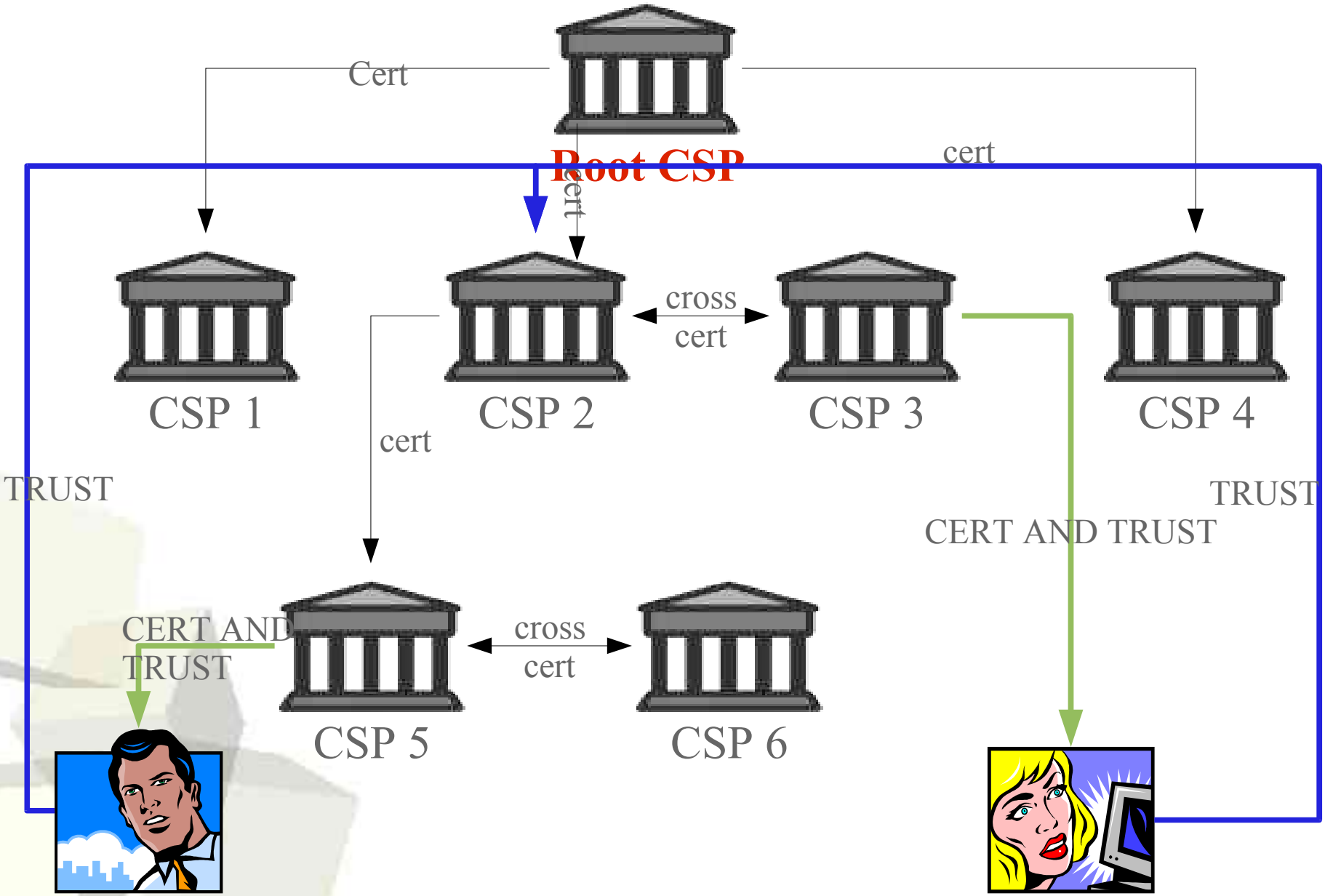
Flat Trust Model (1)



Flat Trust Model (2)

- Small validation paths
- Lists of leaf CAs the user trusts

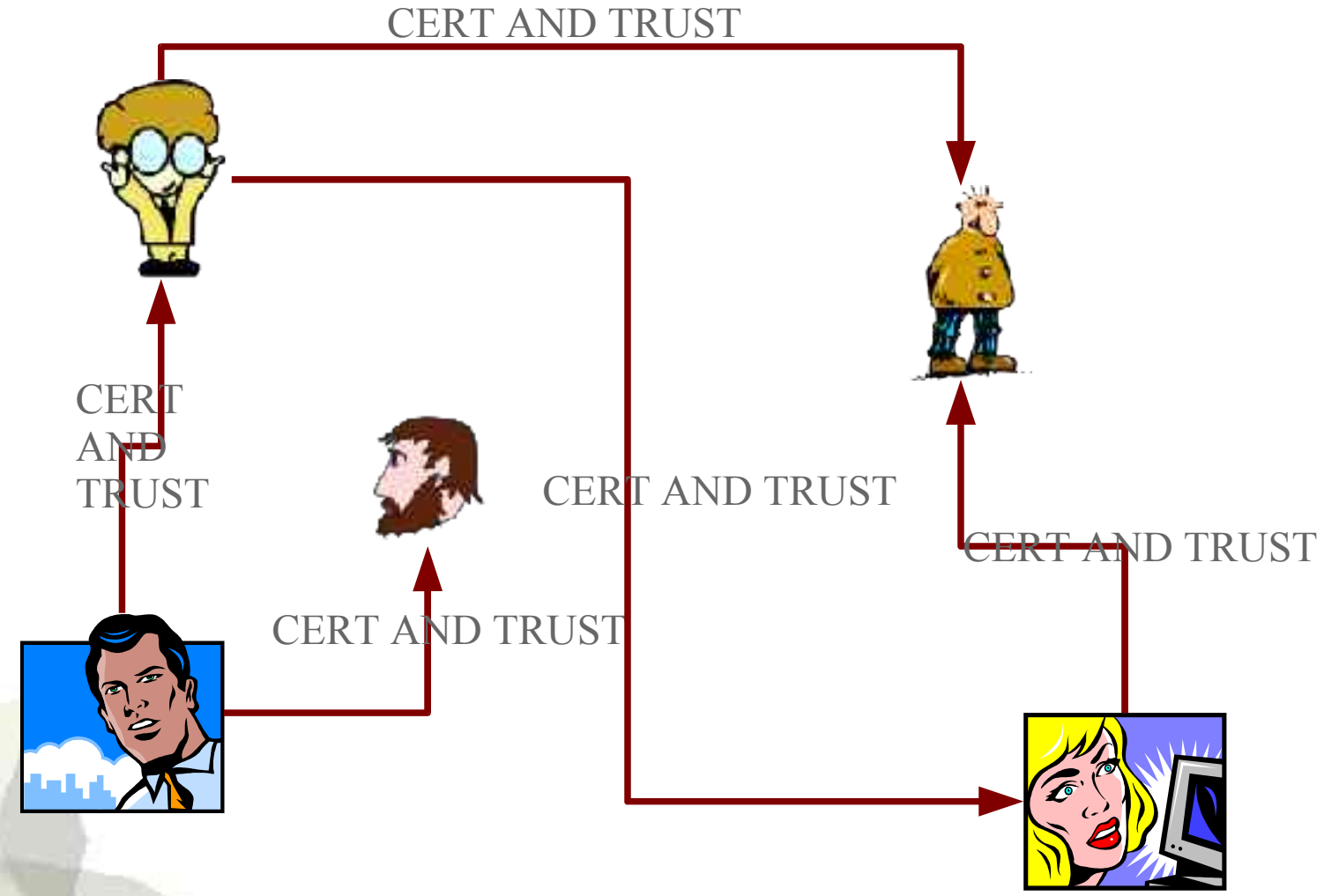
Mixed Trust Model (1)



Mixed Trust Model (2)

- Cross-certifications
- Is it easy to cross-certify?
  - Security Policy
  - Certificate Practice Statements
  - Other issues...

Web of Trust Model (1)



Web of Trust Model (2)

- Not x.509
- Users sign other users' public keys
- PGP

What about certificate revocation?

- EU Directive 1999/93/EC calls for a “secure and prompt revocation service”. Is there one?
- The need for a revocation evaluation framework; research is ongoing
- The need for security awareness programmes
  - Users need to be aware of the PKI potential
  - Dependent entities need to be aware of the risk

Certificate Status Information Mechanisms (1)

- Certificate Revocation Lists
- Compare to Black lists: Banks, Cell phone Operators. Dependent entities: merchants (online POS), Banks, other Cell phone operators
- CRL: Signed list containing serial numbers of revoked or suspended certificates, revocation dates and (optional) revocation reasons

Certificate Status Information Mechanisms (2)

- Authority Key Identifier
- Issuer Alternative Names
- CRL Number
- Delta CRL Indicator
- Issuing Distribution Point
- This update, next update
- CRL Entries
  - Serial numbers of certificates
  - Invalidity date
  - Reason Codes

...Digitally signed by CSP

Certificate Revocation List

- Reason Codes
  - keyCompromise
  - cACompromise
  - affiliationChanged
  - CessationOfOperation
  - certificateHold
  - removefromCRL

Certificate Status Information Mechanisms (3)

- Delta-Certificate Revocation Lists
- Distribution Points
- Fresh Revocation Information (DeltaCRLs on top of Distribution Point CRLs)
- Redirect CRL (dynamic re-partitioning of large Distribution Point CRLs)

Certificate Status Information Mechanisms (4)

- Enhanced CRL Distribution Options
  - Separate location and validation functions.
- Positive CSI
  - CRLs are all wrong… CSI should contain positive info. Dependent entity should set ad hoc freshness requirements and certificate holder should provide ad hoc CSI.

Certificate Status Information Mechanisms (5)

- Online Certificate Status Protocol
  - Server returning signed CSI, corresponding to requests by dependent entities. Possible OCSP Responses:
    1. “Good”, meaning certificate has not been revoked,
    2. “Revoked”, meaning certificate has been revoked or suspended,
    3. “Unknown”, OCSP is not aware of that certificate

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999

on a Community framework for electronic signatures

EU Directive – The Basics

- "This Directive contributes to the use and legal recognition of electronic signatures within the Community;"
- *"Advanced electronic signatures"* (legal recognition, no doubt margin) must be based on
  - *"qualified certificates"*, which are created by a
    - ➔ *"secure signature creation device"*
- Requirements for a CSP to be able to issue "qualified certificates"
  - Meet specific requirements
  - Accreditation by a national authority

EU Directive – Signatures (1)

- "Electronic signature"
  - data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

EU Directive – Signatures (2)

- "Advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

EU Directive – Certificates (1)

- "Qualified certificates" must contain:
  - (a) an indication that the certificate is issued as a qualified certificate
  - (b) the identification of the certification service provider and the State in which it is established
  - (c) the name of the signatory or a pseudonym, which shall be identified as such
  - (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended

EU Directive – Certificates (2)

- "Qualified certificates" must contain (cont.):
  - (e) signature-verification data which correspond to signature-creation data under the control of the signatory
  - (f) an indication of the beginning and end of the period of validity of the certificate
  - (g) the identity code of the certificate
  - (h) the advanced electronic signature of the certification-service-provider issuing it
  - (i) limitations on the scope of use of the certificate, if applicable
  - (j) limits on the value of transactions for which the certificate can be used, if applicable

EU Directive – Secure Devices (1)

- Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
  - (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured
  - (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology
  - (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others

EU Directive – Secure Devices (2)

- Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

EU Directive - Some thoughts (1)

- Directive aims at technology independence
  - **Problem**: Directive identifies requirements that fall under the scope of technology (e.g. secure signature creation devices, Annex III)
  - **Solution**: Define sets of components that comply with the Directive. Caution needed when defining these sets; they must not conflict with other, underlying regulatory frameworks

EU Directive - Some thoughts (2)

- Secure signature creation devices
  - Hardware tokens
    - → easier to deploy
    - → wide acceptance by public as a «secure» method
    - → degree of security awareness required: low
  - Security requirements and evaluation standards
    - → harder to deploy; compliance certification (end-user systems?)
    - → degree of public confidence: low
    - → degree of security awareness required: high

EU Directive - Some thoughts (3)

- Secure signature creation devices – factors to consider:
  - Ease of use,
  - confidence/acceptance by public,
  - cost of implementation, operation and maintenance,
  - security level and assurance,
  - others...

EU Directive - Some thoughts (4)

- Need for «Qualified Value-added Services»
- Should there be a limit on the kind of services CSPs may develop and offer to the public?
- Should we ensure that the new services they will be providing in the future will not damage their impartiality?

PKI Outside Wonderland:

Interacting with the Real World

Section 4: PKI Outside Wonderland

- Where can I use my certificate?
- How come they don't use certificates in... ?
- Food for thought
  - Which CA do you trust?
  - Why is Bob claiming he received a different signed document than the one you 've sent him?
  - Are you sure others cannot masquerade as yourself?
  - Who is that Alice sending you digitally signed emails?
  - Can someone fool Certification Service Providers?
  - Is PKI a cure-all for enterprise-level security?

Where can I use my certificate? (1)

- How come they don't use it for e-banking?
  - EU Directive 1999/93/EC and the national-level laws are just showing their results (qualified certificates)
  - Some Banks had already implemented their own PKI, for e-banking use, before the EU Directive
  - In general, it is probably still too immature to be adopted by the vast majority of Banks
    - Technology issues to be improved yet, e.g. Revocation
    - Banks didn't have a chance yet to try it internally and feel comfortable with it
    - It is not widespread among end users, yet; user education and training might be needed
    - ROI ?
    - Some banks are beginning to consider it; pilot projects underway

Where can I use my certificate? (2)

- How come web sites don't use it for authentication?
  - Privacy issues may be a hindering factor
    - Username/password and a simple registration process provide privacy (one can always refrain from giving up too much personal data during registration)
    - Certificates / qualified certificates cannot provide privacy
    - Attribute certificates could do the job, but then again most of the times you need to identify a specific individual
    - If certs were used, Web site operators would probably have to handle more carefully the stored identification data (Data Protection)
    - Research is being performed, for cert-based mechanisms (e.g. PyTHIA)
  - ROI?

Are they used anywhere at all? (1)

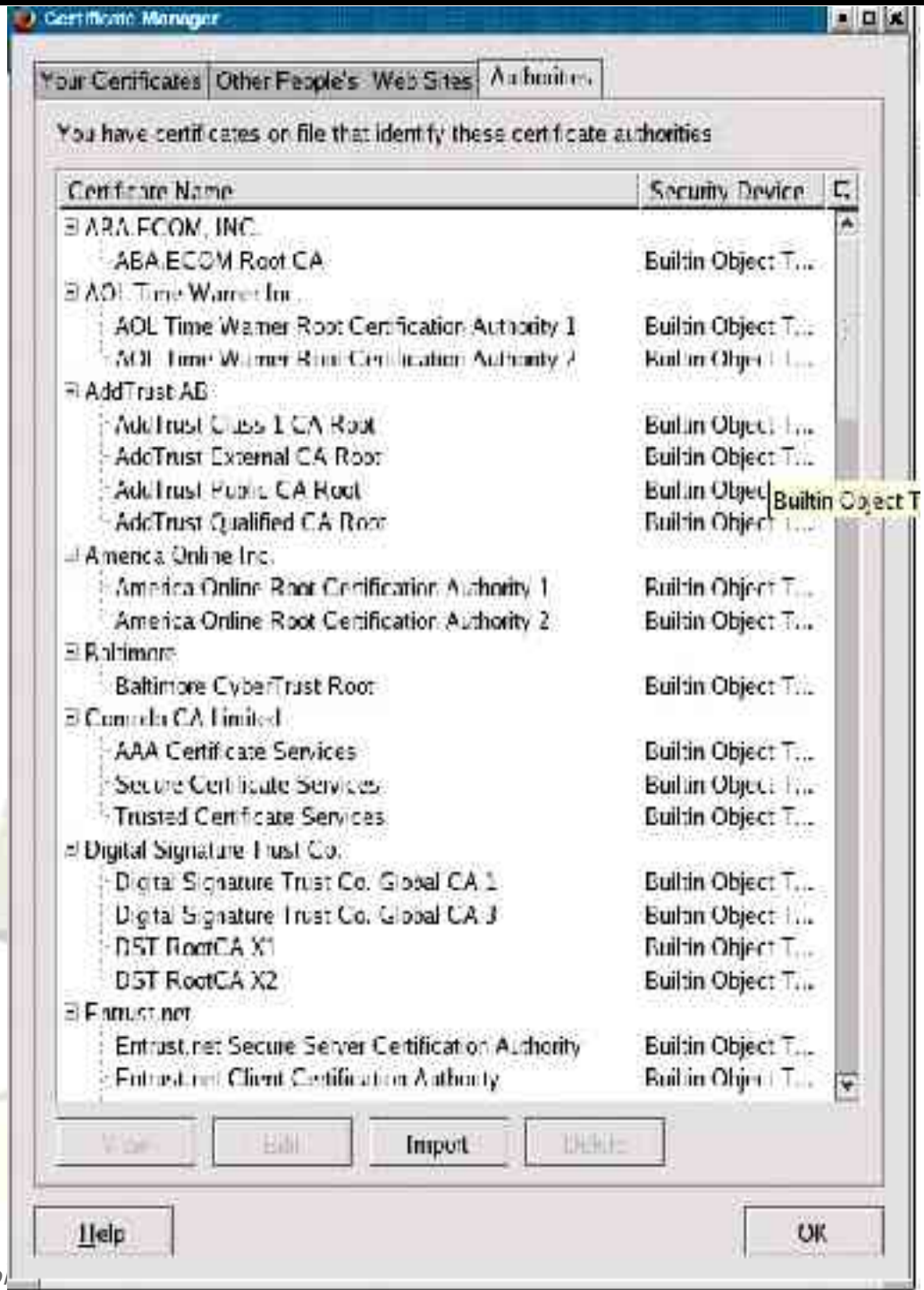
- S/MIME
  - Sign your emails, have others encrypt the ones they send you
- Public sector
  - Could (will?) be the driving force for PKI
  - Pilots (Greece) have already been deployed; soon to be used
- Company-wide
  - Some companies use it internally, to encrypt sensitive emails, sign emails or documents (electronic workflows), or encrypt private users' data. According to the 2004 CSI/FBI Computer Crime and Security Survey, 30% of U.S. Corporations use PKI to enhance their security

Are they used anywhere at all? (2)

- ...let's not forget, before introducing a new technology, one should
  - Identify the need for it
  - Identify the operational risks
  - Estimate and allocate in the budget the operational cost (e.g. PKI key management and administration)
  - Educate the users
  - Await for user acceptance (critical mass), and
  - Estimate the ROI...

Some interesting Problems

Which CA do you trust ?



- How do you pick the CAs to trust?
  - Security Policy
  - CPS
  - Word of mouth
  - Cost of certificate
  - Other criteria?
  - Random

Food for thought (1)

- Where do you store your private key? (EU Directive)
- What is it exactly you are signing?
  - What You Sign is What You See – not there yet
  - Simple PCs (private key outside smart card) and TCB ?
  - Are the Directive's (and national laws') requirements met ?
- The need for information security awareness
  - “Revocation info not available. Proceed?” message - user authentication fatigue
  - “Always check revocation info” option in your browser?

Food for thought (2)

- Identification and naming
  - Global naming?
  - Translation versus transliteration?
- Certificate path validation
  - Who is validating?
  - Do dependent entities understand the implications of the trust model they use?
- Signature policy (underlying legal framework?)
- Revocations
  - Scalability, Transparency, Freshness, Timeliness, ...

Food for thought (3)

- Role of notarisation and timestamping authorities
  - Underlying legal framework?
  - Timely submission?
- Trusted archival services
  - How long should an archive hold info?
  - Who should it be revealed to?
- Use of biometrics in relation to electronic signatures
  - The case of “panic password” versus finger cut-off...

Food for thought (4)

- John asked CA1 to revoke his certificate because his key (smart card) was stolen
- John then uses certificate from CA2 (same public key) to perform transactions and then repudiate
- In the court, John may claim that he didn't know that he had to notify CA2, since only the smart card of CA1 was stolen...

Food for thought (5)

- Enterprise-wide implementations
  - PKI is a solution; identify the problem first
  - Identify and ensure necessary resources are available
    - PKI Administration person-hours
    - PKI Administration procedures
    - Upper management support
  - Procedures for key management, procedures for key management and procedures for key management
  - Archiving/Notarisation
    - What if archive file format becomes obsolete (not supported by newer software versions)?
    - What if specific smart cards / smart card readers become obsolete?

Food for thought (6)

- A typical scenario of solution first, problem identification afterwards

  “We 've got PKI, so we can use the server cert to sign official letters on behalf of the company and e-mail them! What's more, it can be done unattended (bulk signing)!”

- Let's see...
  - Technical problems: are server certs supposed to sign (keyUsage certificate attribute)?
  - Legal problems: Can the server be held legally liable? If not, how can he sign?
  - Yes, please: with unattended signing you 've got to have the private key unencrypted somehow/somewhere, so every employee gets a chance to become a CEO, in turns...

Summing it up

Information Security

- Not about...
  - Secret cryptographic algorithms
  - Obscurity
- About...
  - Risk Analysis
  - Security Policy
  - Changing business problems to security problems (when it comes to crypto, key management problems mostly)
  - Information Security lifecycle
  - User awareness (especially those who need to take decisions; see Top-down approach to security)

Symmetric/Asymmetric crypto: Differences

- A multiple choice test
  - Choice A:
    - ➔ Symmetric is cumbersome; asymmetric is new tech and has many useful features and advantages
  - Choice B:
    - ➔ The difference is in key management; confidentiality of shared key vs integrity (authenticity) of public one
  - Consequences of failing the test
    - ➔ Bad key management ⇨ solutions that increase operational risk
    - ➔ False sense of security

PKI hype

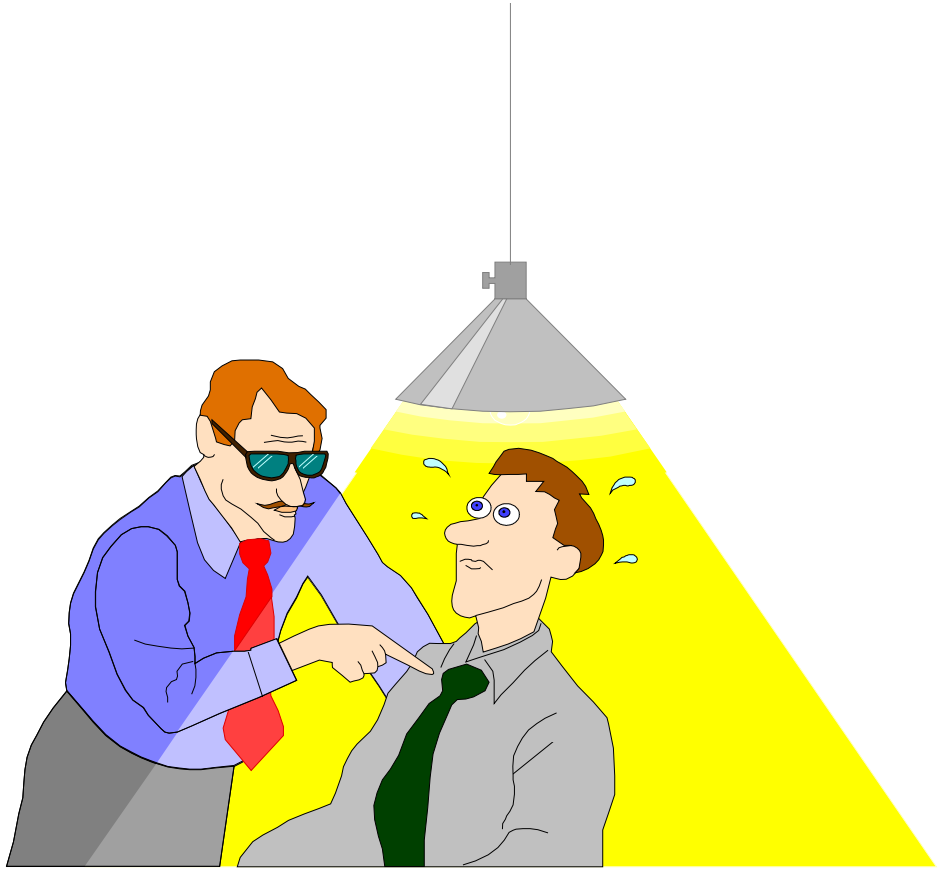
- PKI has still got issues to be resolved
  - Technical (e.g. revocation)
  - Managerial (e.g. enterprise-wide: identify the problem, allocate the resources and then proceed)
  - User awareness (e.g. when you see “no revocation information available currently” there might be stg fishy)
- ...however,
  - End-users seem to be unaware of those
    - ➔ Because we have to start selling PKI/investments have to start paying back?
  - Digital signature laws clearing the path for faster user adoption (and protection) have recently appeared

Taking up an orphan

- PKI is an orphan
  - Science gave birth to a child and gave it up for adoption
  - Few foster parents around, to take up the child before it passes childhood diseases
- PKI is a good solution
  - ...now all we have to do is track down the problem
  - Be careful: easing ulcer pains with aspirin is a bad idea

Do it or dump it ?

- Do it!
  - Childhood diseases are currently being treated
  - Regulatory frameworks in place, allowing for PKI adoption and protecting dependent entities
  - Governments a major driving force (EU)
  - Just remember
    - ➔ Problem first, solution afterwards
    - ➔ PKI or non-PKI, it's about key management, key management and key management



References (1)

- Castell S., User's Requirements for Trusted Third Party Services, INFOSEC Project Report S2101/01, CEC/DG XIII/B6, September 1993.
- W. Diffie, M. E. Hellman, New Directions in Cryptography, IEEE Transactions, vol IT-22, pages 644-654, 1976.
- Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, 13 December 1999, published in the Official Journal of the European Communities, 19 January 2000.
- Gritzalis, S., Spinellis, D. Addressing Threats and Security Issues in World Wide Web Technology, In Proceedings of the 3rd IFIP International Conference on Communications and Multimedia Security, Chapman & Hall, 1997
- Housley R., Ford W., Polk W., Solo D., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, , IETF Network Working Group, Request for Comments 2459 (Category: Standards Track), January 1999, available at http://www.ietf.org/rfc/rfc2459.txt

References (2)

- ISO Standard 11770 (1996), Information Technology - Security Techniques - Key Management - Part 1: Framework.
- ITU-T Recommendation X.509 (1997) and ISO/IEC 9594-8:1997, Information technology - Open Systems Interconnection, "The Directory: Authentication framework".
- J. Iliadis, D. Spinellis, S. Katsikas, D. Gritzalis, B. Preneel. "Evaluating Certificate Status Information Mechanisms". In Proceedinds of the 7th ACM Conference on Computer and Communication Security: CCS '2000, pages 1-8. ACM Press, November 2000
- Kohnfelder L., Towards a practical public-key cryptosystem, BSc Thesis, M.I.T., Cambridge MA, September 1978.
- PKITS, CEC-DGXIII-ETS-II project 23192, Deliverable D3 “Public Key Infrastructure with Timestamping Authority”, April 1998.

References (3)

- Ronald L. Rivest, Adi Shamir, Leonard M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, vol21, No2, pp.120-126, 1978.
- Rivest R., Can We Eliminate Revocation Lists?, In Proceedings of Financial Cryptography 1998, available at http://theory.lcs.mit.edu/~rivest/revocation.ps
- Schneier B., Applied Cryptography, 2nd ed, John Wiley & Sons, 1996.
- Zhou J., Gollmann D., A Fair Non-repudiation protocol, Proceedings of the 1996 IEEE Symposium on Security and Privacy, pp.55-61, IEEE Computer Society Press, May 1996.
- Zhou J., Gollmann D., An Efficient Non-repudiation protocol, Proceedings of the 10th IEEE Computer Security Foundations Workshop, pp.126-132, IEEE Computer Society Press, June 1997.