University of the Aegean

De Facto Joint Research Group

PKI: Is it worth something, or what?

John Iliadis[1,2], Stefanos Gritzalis[1]

[1]Department of Information and Communication Systems Engineering
University of the Aegean
E-mail: {jiliad,sgritz}@aegean.gr

[2]Department of Informatics
Technological Educational Institute of Athens
E-mail: jiliad@cs.teiath.gr

Overview

- Communication Networks: Now and Then.
- Symmetric Cryptosystems versus Asymettric Cryptosystems
- Applications of Asymmetric Cryptosystems
- Facing Threats in Electronic Transactions
- Certification Service Providers, (a.k.a. Certification Authorities, a.k.a. Trusted Third Parties ???)
- EU Directive on Digital Signatures
- Further Research on PKI
- Conclusions

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Communication Networks: *Now* and *Then*

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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Communication Networks:

Now and *Then* (cont.)

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

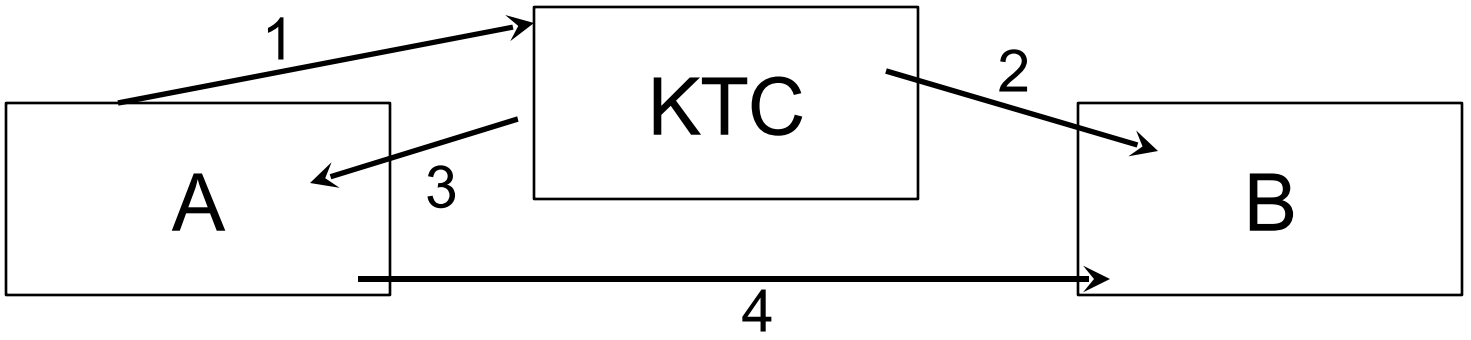
John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution - Symmetric Cryptosystems

- Direct
- Key Translation Center
- Key Distribution Center
- Based on asymmetric techniques
  - secret key agreement
  - secret key transport

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

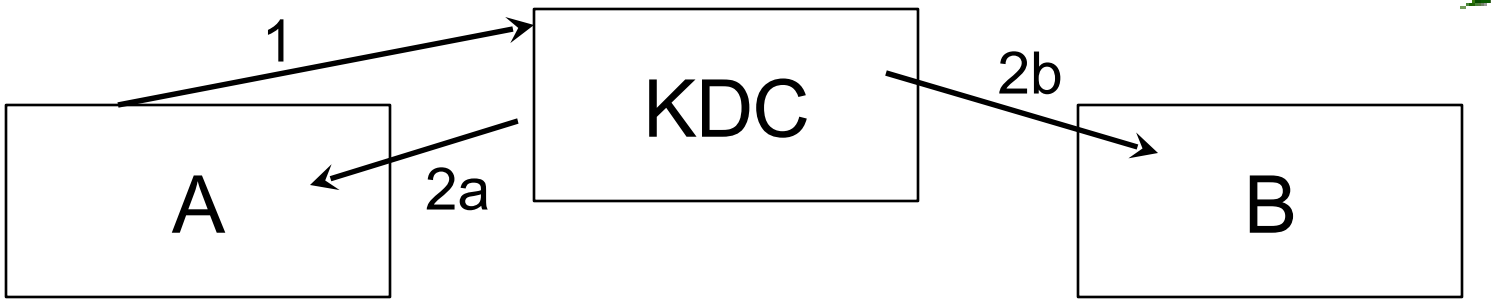
Key Translation Center (symmetric crypto)



- A->KTC: enciphered key
- KTC->B: sends B re-enciphered key, **OR**
- KTC->A: sends A re-enciphered key
- A->B: A sends B re-enciphered key

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution Center (symmetric crypto)



- A->KDC: request for shared key
- KDC->A: sends A enciphered shared key
- KDC->B: sends B enciphered shared key

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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution in Symmetric Cryptosystems A Note

- All mechanisms require the existence of a shared symmetric or asymmetric key and an inline Key Center.

Centralised
Closed
Private
Proprietary protocols
Expensive

Distributed
No ownership
No central control
Resilience
Access to anyone
Standardised protocols
Low-cost access.

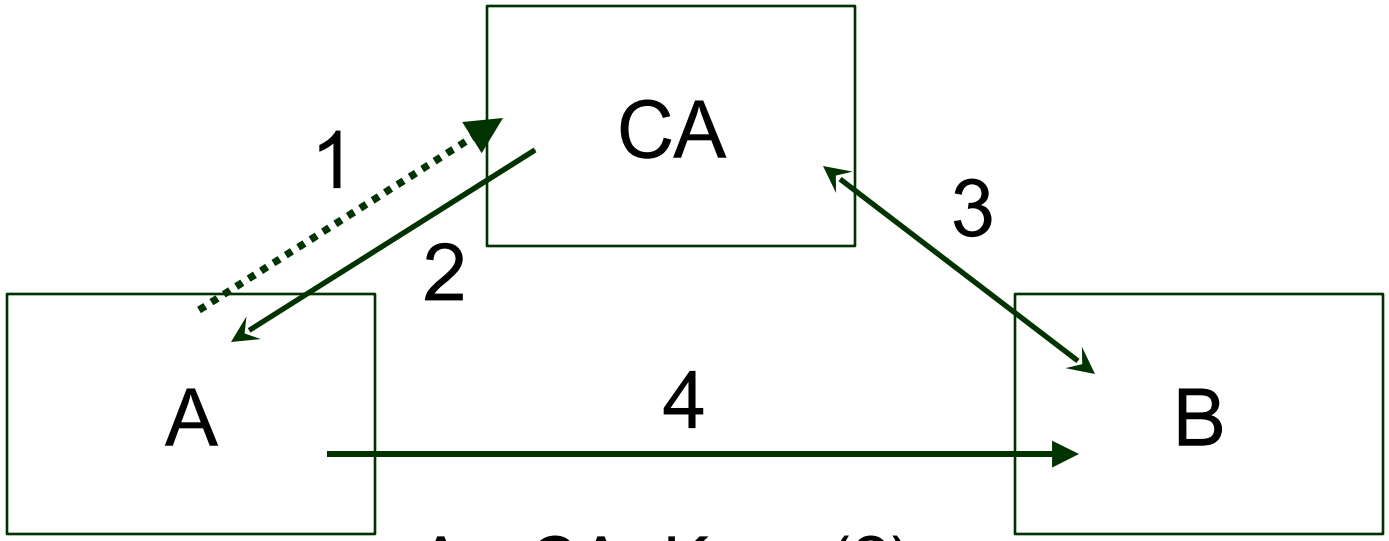
John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution: Asymmetric Cryptosystems

- Protected channels (data origin authentication and data integrity protection, e.g. courier and registered mail)
- CSP-assisted (i.e. certificates)

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution: Asymmetric Cryptosystems (cont.)



- A->CA: Key_A (?)
- CA->A: $Certificate_A$
- CA<->B: $Certificate_A$ or $Certificate_{CA}$
- A->B: $Certificate_A$

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution in Asymmetric Cryptosystems - A Note

- Mechanisms require the existence of either an integrity protected channel, or at least an offline CSP*

Centralised	Distributed
Closed	No ownership
Private	No central control
Proprietary protocols	Resilience
Expensive	Access to anyone
	Standardised protocols
	Low-cost access.

*Other CSP operational requirements, like revocation, necessitate the online operation of CSPs

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution: A Final Note

The Case of Asymmetric versus Symmetric Cryptosystems, and vice-versa.

Verdict: *Innocent on all charges*, both of them.

- there are applications that necessitate symmetric crypto, like small scale closed networks, top-secret communication lines (one-time pads), requirements for fast encryption (e.g. slow processor speeds: smart cards) etc.
- there are applications that necessitate asymmetric crypto, like applications over communication channels where one cannot protect the confidentiality of the exchanged messages (key distribution?)

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution: A Final Note (cont.)

The Case of Asymmetric versus Symmetric Cryptosystems, and vice-versa.

Verdict 2: *The Case should never have been taken to court!*

- There's no point in excluding either one of them. Joint usage leads to best results (e.g. Digital Envelopes, asymmetric based distribution of symmetric keying material).
- There are advantages and disadvantages in both. The main difference is in *key management requirements: confidentiality against authenticity*

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Key Distribution: A Final Note (cont.)

Asymmetric crypto was not invented to meet the needs of new, distributed and loosely federated networking environments. It existed before.

It has been *a solution in search of a problem*…

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Digital Certificates

Offline authentication token

Third, trusted entity vouches for it

Expiration, revocation

Contents:

- identification info of certificate holder
- identification info of CA
- public key of certificate holder
- expiration date
- other info (e.g. CSI location info)
- signed by CA

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Digital Signatures

- Generating certificate-supported signatures
- Non-repudiation
  - Timestamping
  - Non-repudiation mechanisms
  - Underlying legal framework

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Some Threats in Electronic Transactions

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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Insecure Electronic Transactions

insecure communication channel

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Facing Threats

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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Facing Threats (cont.)

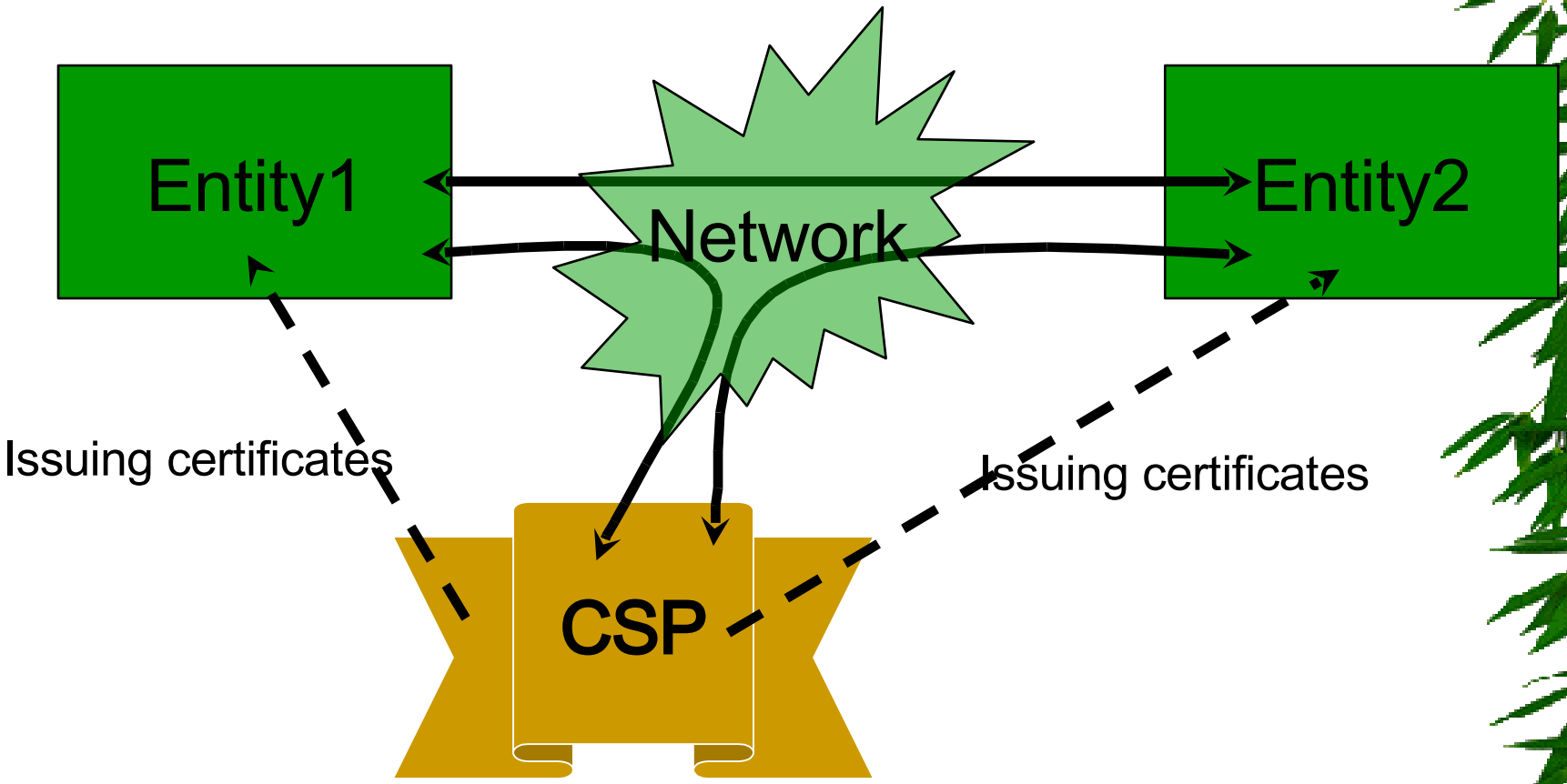
Masquerade - Web spoofing
Exchange of X509v3 certificates and verification against a Directory

Password stealing
Passwords are never transmitted in the network

Unauthorised access
Local ACL. Authentication by certificate verification

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Securing electronic transactions



John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSP : The Cornerstone of PKI. *An Overview*

- *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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

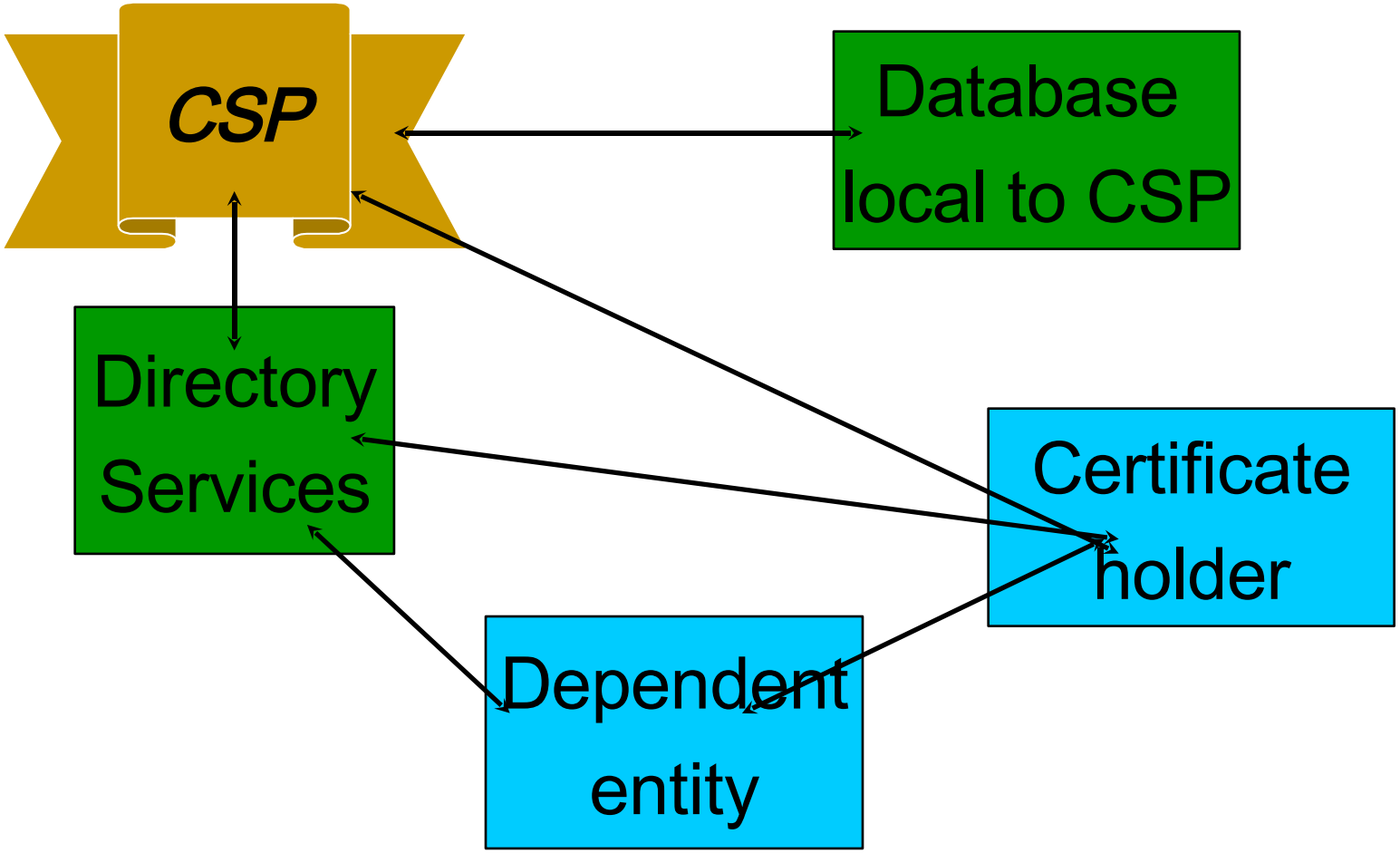
CSP : The Cornerstone of a Public Key Infrastructure. *Technical Infrastructure*

JRG
JOINT RESEARCH GROUP ON COMMUNICATION AND INFORMATION SYSTEMS SECURITY

- *Certification Authority,* providing certificates.
- *Registration Authority*, registering users and binding their identities to certificates.
- *Repositories,* storage and dissemination entities containing CSP-related public material such as certificates and CRLs.
- *Certificate holders,* holding certificates issued from Cas, which they use in order to sign or authenticate themselves.
- *Dependent entities,* entities that use the certificates presented by other certificate holders in order to authenticate the latter or verify their signature.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSP : The Cornerstone of a Public Key Infrastructure.
Technical Infrastructure



John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSP services and functions

- *Electronic Registration*
- *Key Personalisation, Generation, and Repository*
- *Certificates: Structure, Generation, Distribution, Storage, and Retrieval*
- *Certificate Directory Management*
- *CRLs: Structure, Generation and Maintenance, Distribution, Storage, and Retrieval*
- *Auditing*

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

PKI

- Set of CSPs
- Interoperability and corroboration
- Legal framework
- Value-Added services
  - Timestamping
  - Information Archiving
  - Notary Public
  - ...

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

European Directive on Electronic Signatures

JRG
JOINT RESEARCH GROUP ON COMMUNICATION AND INFORMATION SYSTEMS SECURITY

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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Secure Signature Creation Devices (cont.)

- Factors to consider:
  - Ease of use,
  - confidence/acceptance by public,
  - cost of implementation, operation and maintenance,
  - security level and assurance,
  - others...

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Areas needing further research

- Identification and naming (global naming? translation versus transliteration?),
- Certificate path validation (who? trust model?),
- Signature policy (underlying legal framework?),
- Scalable revocations and scalable suspensions (scalability, transparency?).

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Areas needing further research (cont.)

- Role of notaries 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 (beware: “panic password” versus finger cut-off…).

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Some interesting problems to be studied

Certificate 1	Certificate 2
John Doe	John Doe
org: X	org: Y (X?)
Country: GR	Country: GR

In general, TTP service-level collaboration has to be studied further

- cross-certification (technical, legal)
- revocation
- ...

Qualified Value-added Services

- 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?

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Fashion and PKI

Current commercial PKI 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!

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Fashion and PKI (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

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Fashion and PKI (cont.)

- Requirements->Services->Functions ->Implementation
- Certificate and Security Policy of CSP
- Legal framework and regulations
- Complexity in design and development
- User-awareness needed
- Low user-acceptance
- Clearly not an InfoSec bandage

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Conclusion

PKI is a panacea for security as much as aspirin is a panacea for pain.

Easing ulcer pains with aspirin SHOULD BE AVOIDED AT ALL COSTS...

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002