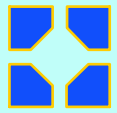
Electronic Commerce & Payments on the Internet



SEMPER

A security framework for electronic commerce

ACTS

Gérard LACOSTE
SEMPER Project Manager
Centre d'Etudes et Recherches IBM France
La Gaude

E-mail lacoste@vnet.ibm.com

Agenda

431LG052

1. Secure commerce

2. SEMPER project

3. Cross-border commerce

Friendly electronic commerce: a great challenge to security

431LG052

- **Friendliness**
  - Ease of use
  - Ubiquitous software
  - Open access
- **Trust**
  - Identification of users
  - Negotiations
  - Reliability
- **Security**
  - Preserve transaction integrity
  - Ensure Privacy
  - Be legally predictable

Electronic commerce must be as friendly and secure as the traditional marketplace, or more!

Electronic commerce users need to become aware of threats

431LG052

Threats against sellers

- No payment
- No legal status of orders
- No receipts of delivery
- Fake orders from fake customers
- Loss of reputation by fake servers
- Unauthorised data access
  - » keys
  - » dishonest competition
  - » confidential customer data

Threats against buyers

- order hijacking
  - » payment against nothing
  - » denial of service
- loss of privacy
  - » behaviour
  - » preferences
- unauthorised access
  - » keys
  - » credit information

Resolution of organizational issues is key to remove uncertainty

- **Issues**
  - High complexity of security technology
  - Trust
  - Interoperability
  - Legal uncertainty
  - Public key infrastructure
  - Cryptography
  - Training of users
- **Status**
  - Piecemeal progress
  - First good signs
    - » consensus on SET
    - » integration of Web sites with existing systems

It is becoming urgent to organize the electronic marketplace!

SEMPER: a systematic approach of the secure marketplace

431LG052

- **Open security framework**
  - Model of the electronic marketplace
  - Open and generic security architecture
- **Security services**
  - Basic services
  - Advanced services
- **Validation**
  - Prototype
  - Field trials
- **Dissemination**
  - Requirements, guidelines
  - SEMPER specifications
  - Demonstrations

» G7
» standardisation committees
» scientific community
» public

SEMPER: a representative set of European experts

Service provision

- Otto Versand
- Eurocom
- Fogra
- Maris

Banking

- Europay
- Commerzbank

Telecom operators

- France Télécom
- KPN Research
- Intracom

Social sciences

- Freiburg Univ.

Security engineering

- Cryptomathic
- CWI
- Digicash
- GMD
- IBM
- r^3
- SINTEF
- Dortmund Univ.
- Hildesheim Univ.
- Saarbrücken Univ.

SEMPER shapes an open architecture for best acceptance

431LG052

- **Model of the marketplace**
- **Open architecture**
- **Ubiquitous software**
- **System-level architecture**
- **Multi-party security**

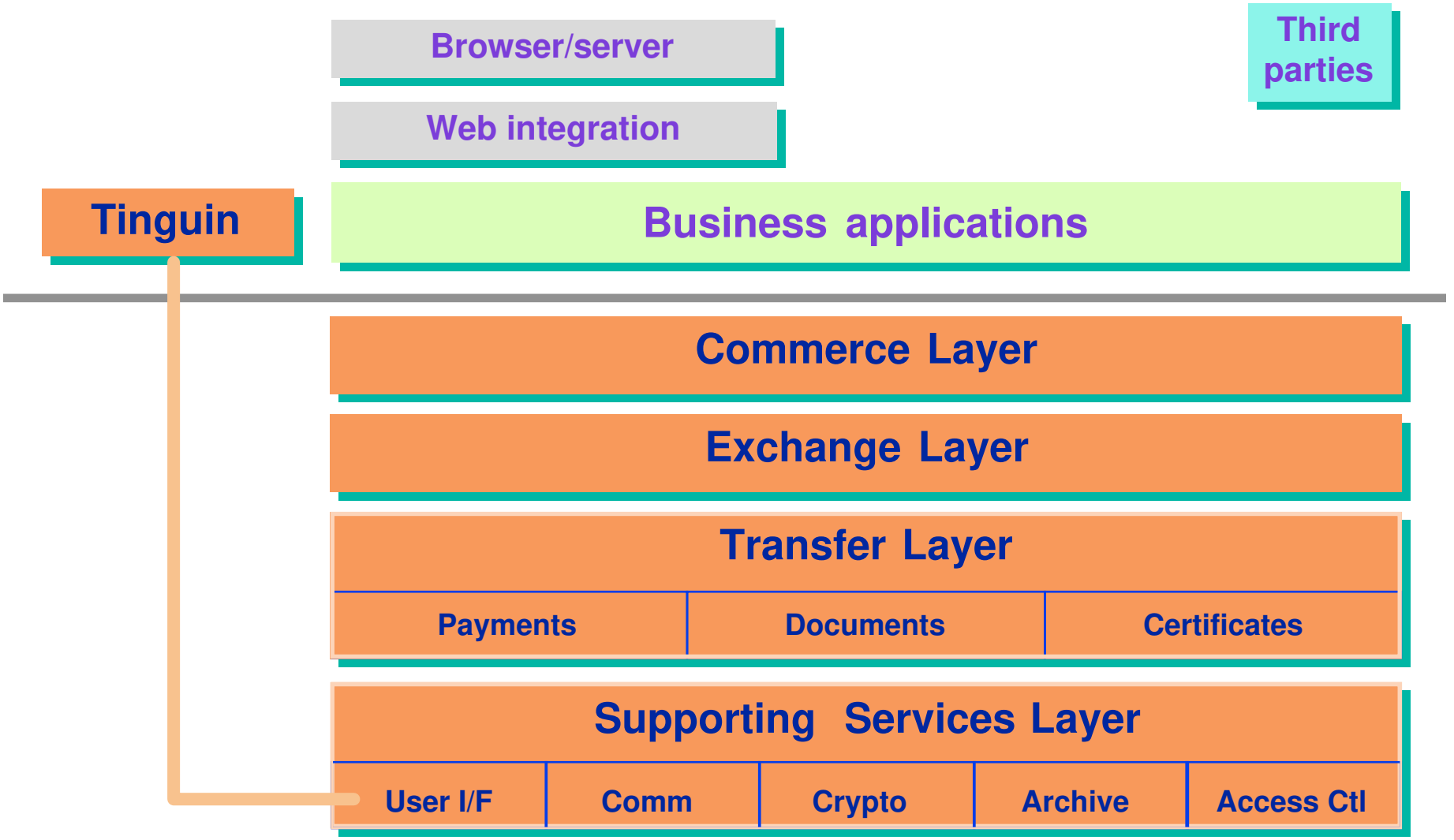
SEMPER builds on fundamental standards

431LG052

- **Portability** — **Java**
- **Communication** — **HTTP**
- **Payment** — **SET, Ecash, E-check**
- **Certification** — **X.509**
- **Cryptography** — **DES, RSA**
- **Transport** — **TCP/IP**

SEMPER proposes a layered security architecture

431LG052



SEMPER makes users aware of critical information

431LG052

Trusted user interface

Connected to ACTIMEDIA

Offe
r
BACH Preludes
BEETHOVEN Piano Sonatas

Price	750 FF
VAT tax	50 FF
Shipping	70 FF
TOTAL	870 FF

Signed May 25, 1997 14:00

ORDER SIGN PAY

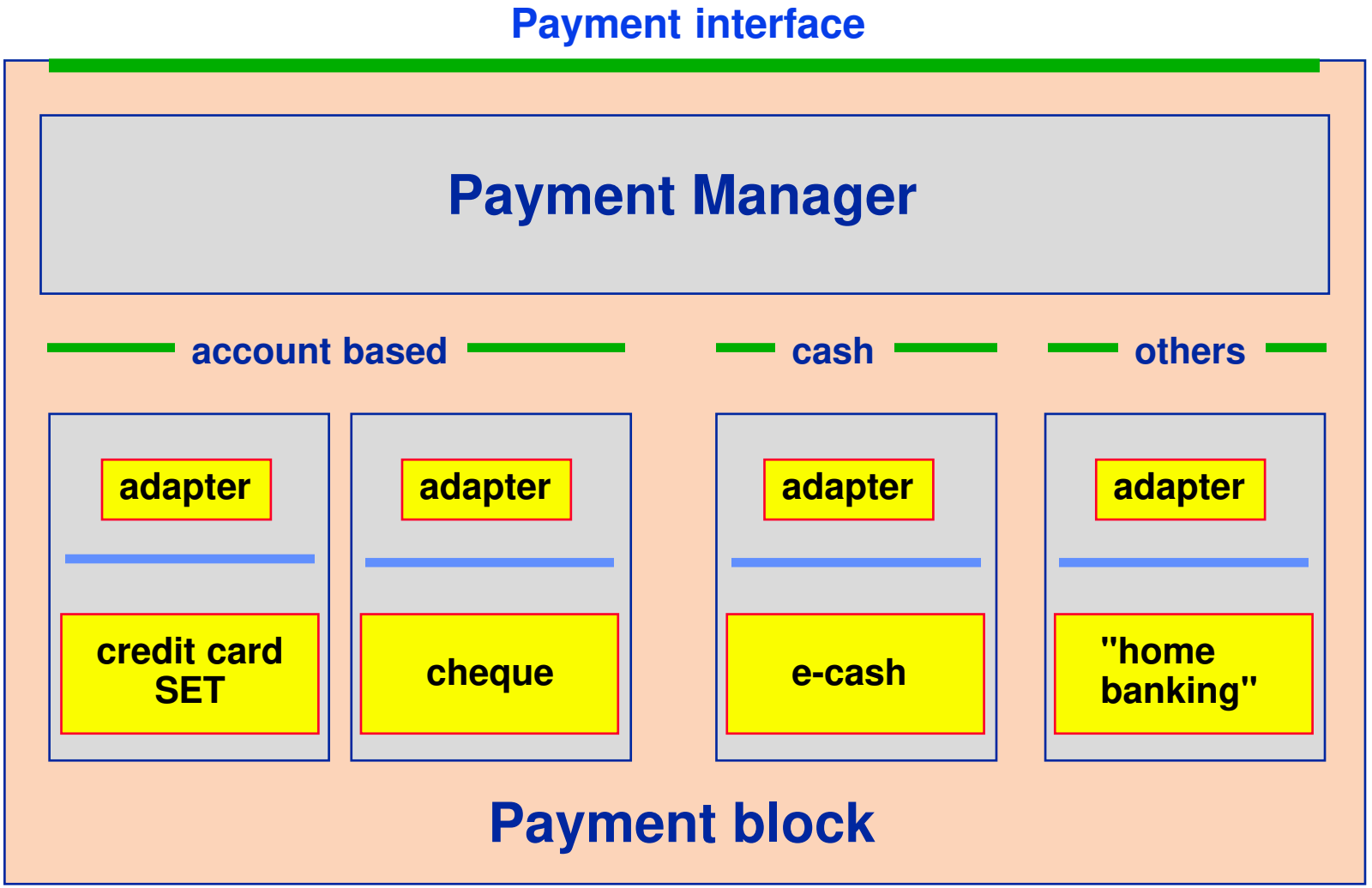
Browser window

Classical Music

☐	BACH Suites for violin	200 FF
☑	BACH Preludes	250 FF
☐	BACH Partitas	400 FF
☐	BEETHOVEN Trios	400 FF
☑	BEETHOVEN Piano Sonatas	500 FF
☐	BEETHOVEN Sonatas	700 FF
☐	COUPERIN	400 FF

SEMPER openness: the payment block

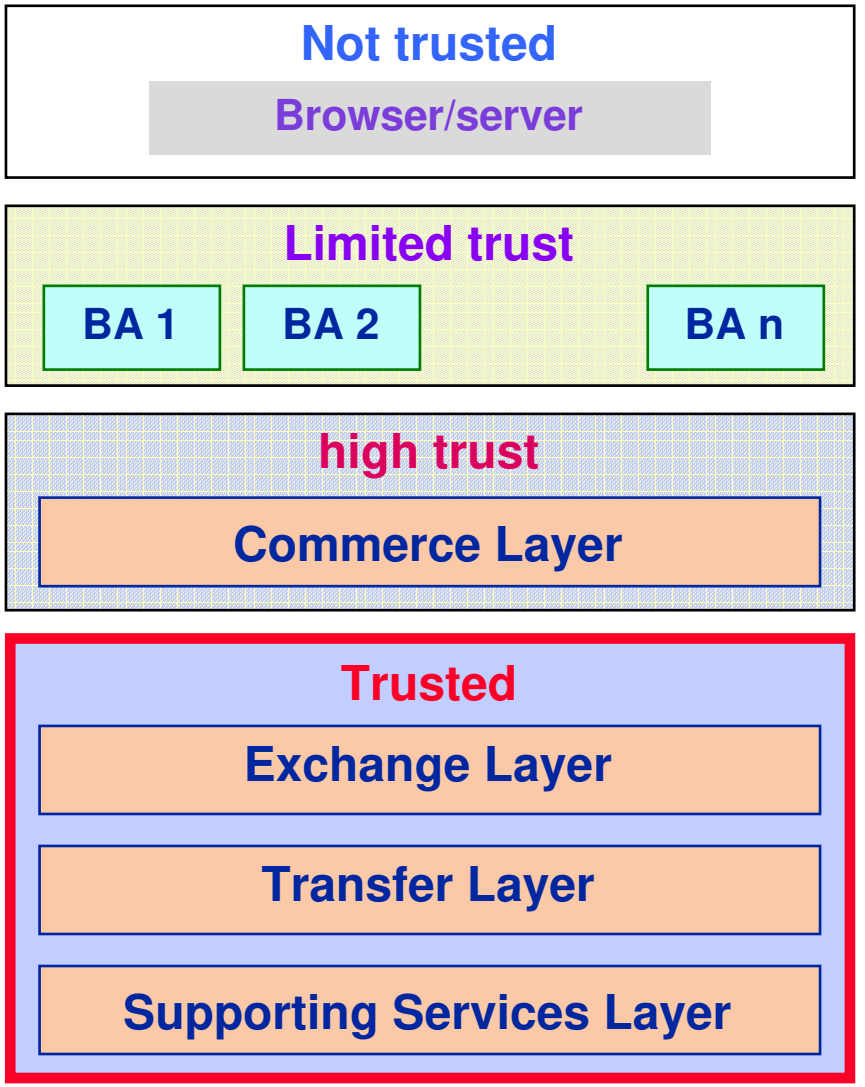
431LG052



SEMPER architecture addresses multi-party security

431LG052

- **Multi-party security**
  - Buyers
  - Service providers
  - Banks
  - RA/CA authorities
  - Notary public
  - Arbiters
- **Trust hierarchy**
  - Browser/server
  - Signed business applications
  - Commerce Layer
  - System kernel



BA Business Applications RA/CA Registration and Certification Authorities

SEMPER offers security services for today and for tomorrow

431LG052

Basic services

- Authentication
- Signed offer
- Signed order
- Payment
- Signed delivery

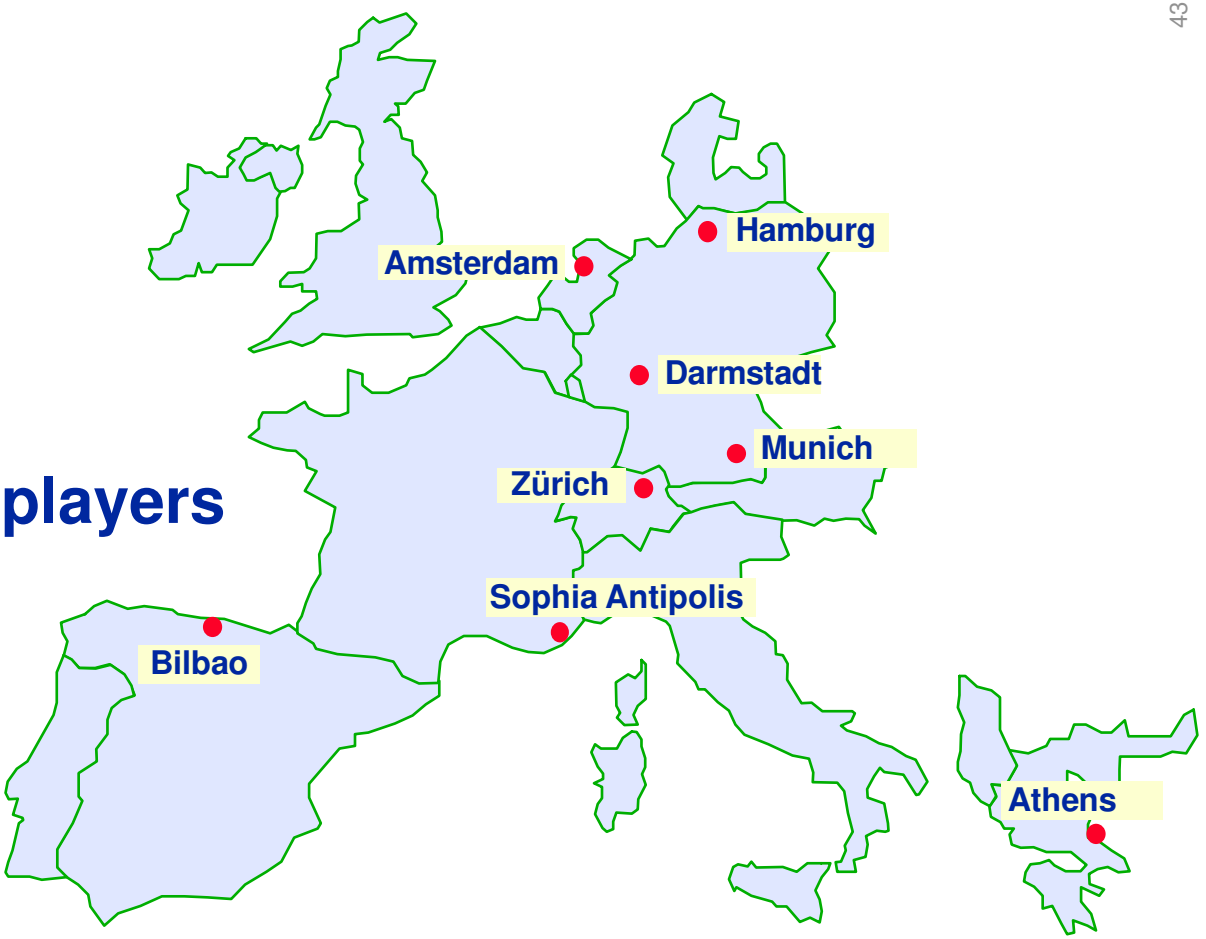
Advanced services

- Fair exchange
- Secure document handling
  - » Certified mail
  - » Contract signing
  - » Credentials
  - » ...
- New payment instruments
  - » Electronic cheques
  - » Stored-value cards
- Anonymity
- Resolution of disputes

SEMPER validation relies on a rich set of trials

431LG052

- **Business contexts**
  - Distance learning
  - Mail order
  - Library
  - Travel
  - Image processing
  - Software localisation
- **Electronic commerce players**
  - Buyers
  - Sellers
  - Banks
  - RA/CA authority
- **Payments**
  - SET
  - Ecash
  - Chipper



SEMPER collects useful indicators from initial experiments

- **Basis**
  - Sites opened and in preparation
  - Basic services only
- **Results**
  - Buyers
    - » Trusted user interface provides much comfort, needs to be more friendly
    - » Education and training is a strong requirement
  - Sellers
    - » Concerned mainly by payment issues
    - » Underestimation of integration efforts
  - Banks
    - » Integration of electronic payment instruments raises difficulties
    - » Cross-border electronic commerce poses legal issues
  - Technology
    - » No architectural problem for trials implementation
    - » Access to more accurate requirements on Commerce Layer and Trusted user interface

Users uncertainty grows with international electronic commerce

431LG052

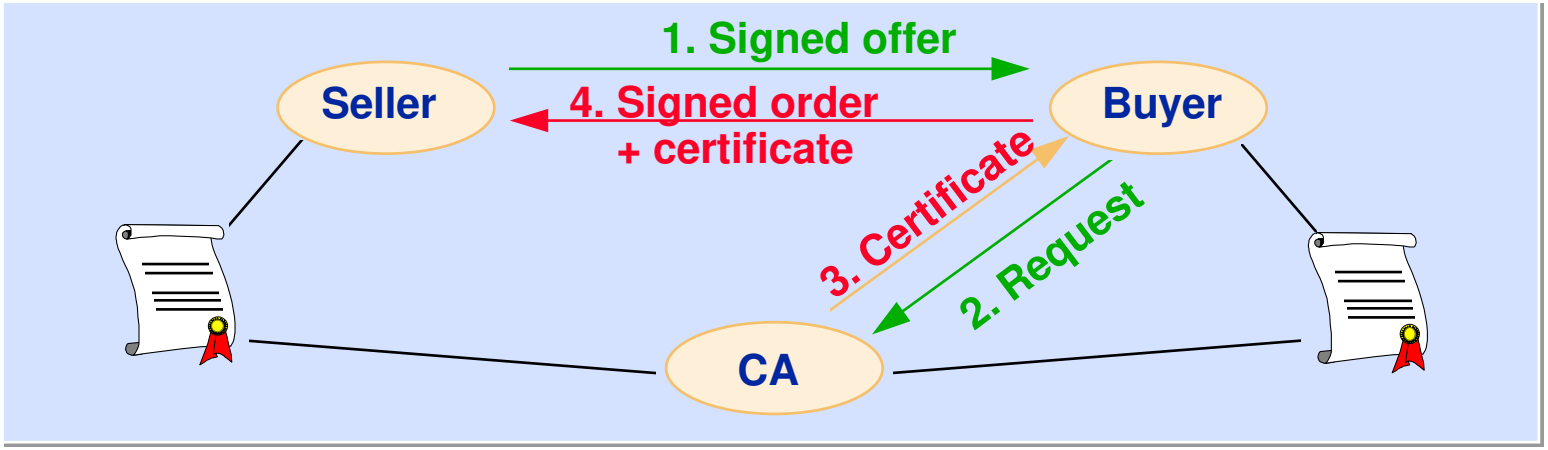
- **Patchwork of laws across countries**
  - Users are not trading experts
  - Different, contradicting, laws
    - » Advertising
    - » Sales practices
    - » Intellectual property rights protection
    - » Privacy
  - Legal jurisdictions
    - » Applicable law may be selected by the parties
    - » Buyers cannot be deprived from their home country protection
    - » Jurisdictions of convience may appear
- **Unclear legal status of technology**
  - Cryptography
  - Digital signatures
  - Electronic records

Routine international electronic commerce requires a well-defined legal framework

SEMPER agreements reduce uncertainty

431LG052

- **Model**
  - Third party (CA) agreements signed on paper by sellers and buyers
  - Agreement limits buyers' liability
  - CA's certificates ensure buyers' liability



- **Benefits**
  - Buyers are protected against potentially high loss
  - Sellers can safely enlarge their market share

A step towards a well-defined legal situation for routine international electronic commerce

SEMPER is leading the way to the secure marketplace

431LG052

The global secure electronic marketplace requires

a security framework

NOW

SEMPER

is making global secure electronic commerce

POSSIBLE

http://www.semper.org