The
SEMPER Electronic Commerce Agreement

2nd Public SEMPER Workshop
Rüschlikon, Switzerland, November 4th 1998
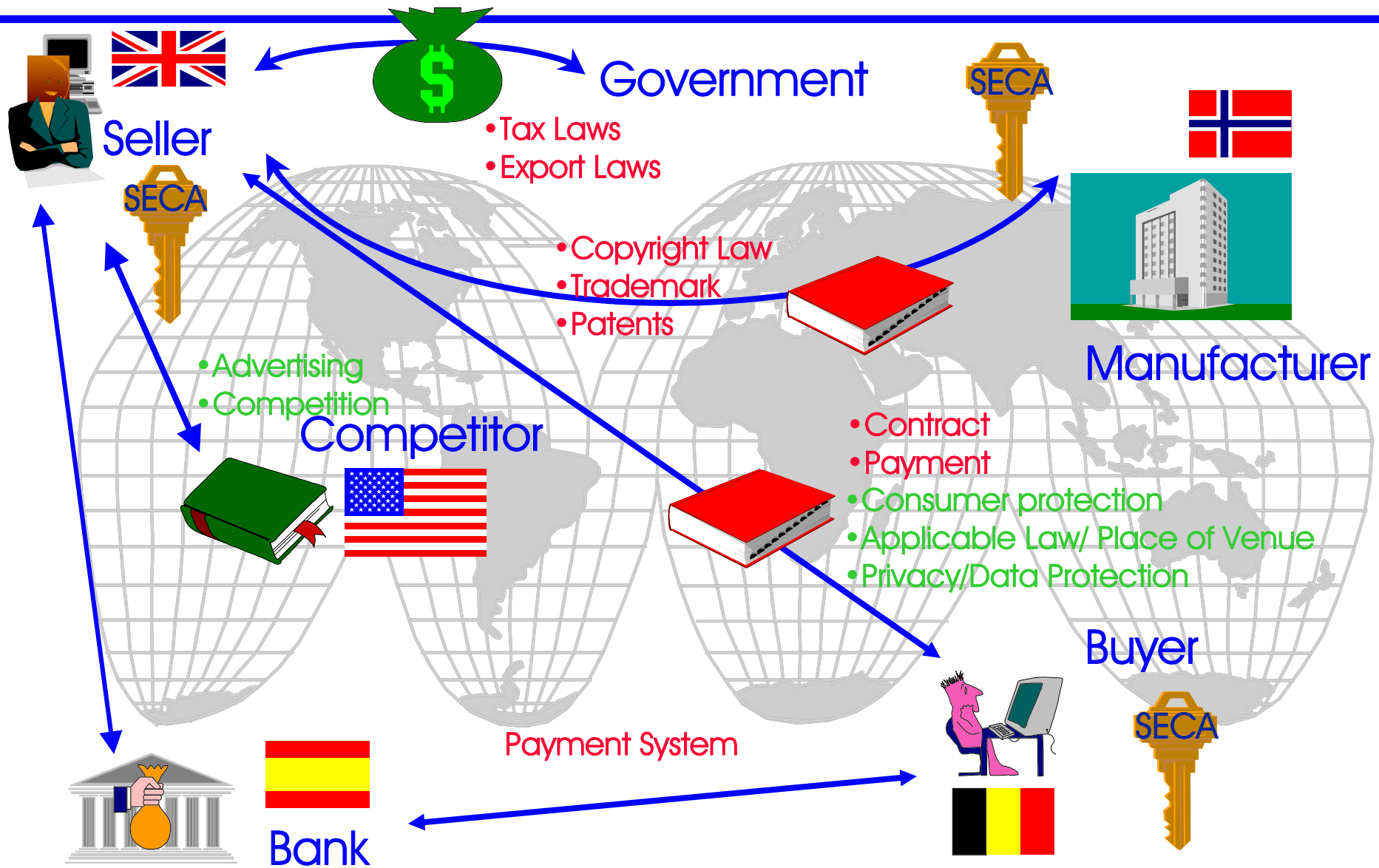
SEMPER

security engineering

Rita Zihlmann
Entrust Technologies Europe   r3 security engineering ag
rita.zihlmann@entrust.com

1

Current Situation in Electronic Commerce

Policy

Contract between CA's

Policy

CA 1

CA 2

Base Contract

Bank

Buyer

784.23.123.456

P. Muster

Seller

Bank

Electronic Money Provider
Credit Card Organization

Clearing

SEMPER

2
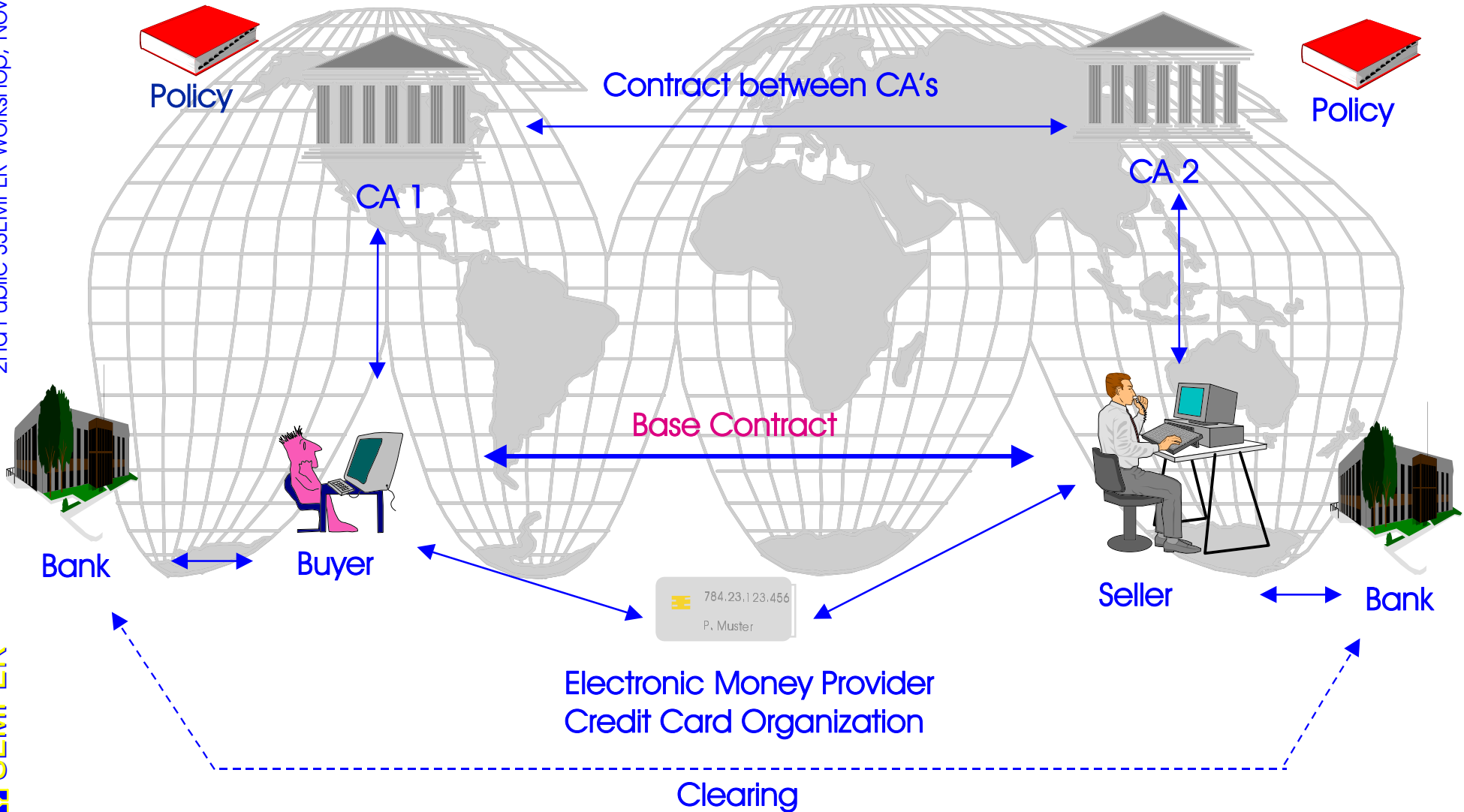
Situation in Electronic Commerce with SECA

Policy

Contract between CA's

Policy

SEC CA 2

SECA CA 1

SECA

§§§§

signature

Bank

Buyer

Supplier

Bank

784.23.123.456

P. Muster

Electronic Money Provider
Credit Card Organization

Clearing

3
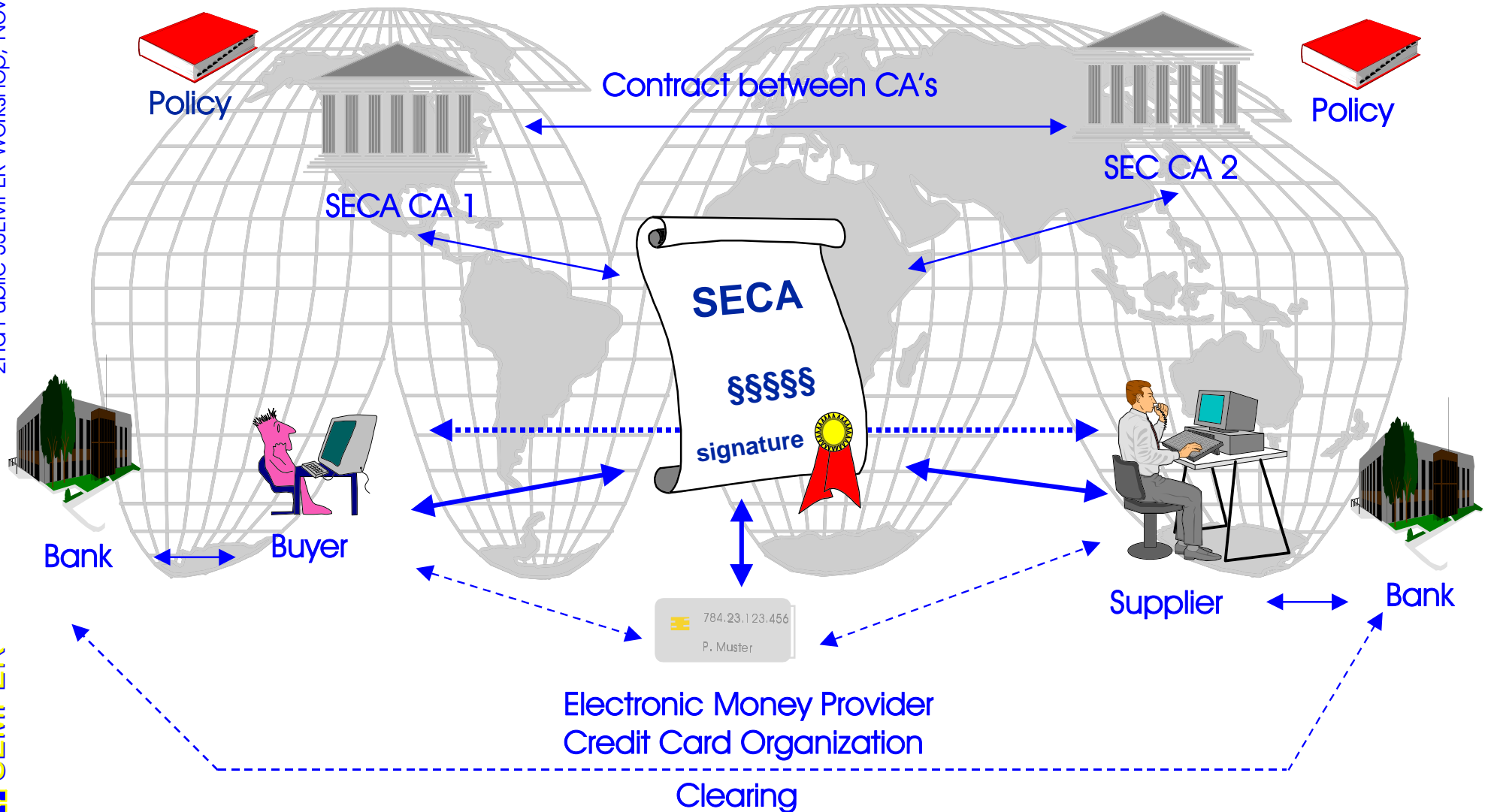
Scenario of a Business Transaction over Open Networks

SEMPER

Seller

SECA

Government
- Tax Laws
- Export Laws

SECA

Manufacturer

- Copyright Law
- Trademark
- Patents

- Advertising
- Competition

Competitor

- Contract
- Payment
- Consumer protection
- Applicable Law/ Place of Venue
- Privacy/Data Protection

Buyer

Payment System

SECA

Bank

4

Main Obstacles to Electronic Commerce

- Various legal systems with individual regulations

- Without Digital Signatures players do not trust in Electronic Commerce

- No unified requirements for CA's and no harmonized CPS

- No or not sufficient regulations on liability for digitally signed messages

SEMPER

Focus of the Selected Approaches

UNCITRAL Model Law (1996) →
- Functional equivalent of digital signatures to traditional signatures
- No regulations on Liability

OECD Guidelines (1992) →
- General recommendations for electronic commerce and for liability

EU Directive
(Proposal 1998) →
- Validity of Digital Signatures
- Liability of CA's
- Mutual recognition of certificates

German Digital
Signature Act (1997) →
- Establishing a secure infrastructure for digital signatures
- Licensing of CA's
- Liability of CA's for issuing certificates

Utah
Digital Signature Act (1995) →
- Building of a CA
- Duties and liabilities of a CA
- Duties and liabilities of the subscriber

EDI Agreements →
- Legal Protection on a bilateral commercial relationship

SEMPER

The Principles and the Solution of SECA

SECA

§§§§

signature

➡ **Principles**

- Establishment of a well defined legal basis for players doing electronic commerce

- Regulate liability for digital signatures

- Enable fair cross-border commerce between b-b, b-p and p-p, including non technical players

- Enhance awareness of the players

➡ **Solution**

- Agreement with provisions of liability among other provisions

- Liability limit for claimed compromised keys

- Code of Conduct that has to be followed, including defaults

- Guidelines with criteria for electronic commerce software

SEMPER

The Structure of SECA

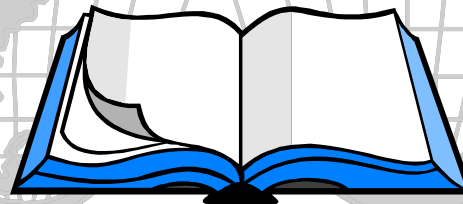1. 'The Agreement'

SECA

§§§§§

signature

- provisions
- handwritten signature of the player
- deposit at the SECA CA

2. 'Code of Conduct'

Behavior related to business

3. 'The Guidelines'

- Requirements for technical equipment
- 'SECA compliant' components
- Protection from attacks

'The Agreement'

SECA

§§§§§

signature

Agreement between the SECA player and the SECA CA with effect to other SECA players or non-SECA players

Scope of Agreement

- Acting according SECA whenever player uses or offers to use the SECA key for signing digitally
- Area of applicable business transactions
- Obligations of the SECA Players

Formation and Validity of Contracts

- Applying SECA defaults
- Validity of digitally signed contracts
- Assent of digital signatures

Liability

- Liability for digitally signed messages
- Liability for claimed compromised keys
- Liability of CA's and Manufacturers
- Liability limits

Breach of Agreement

- Exclusion from SECA
- Blacklists

SEMPER
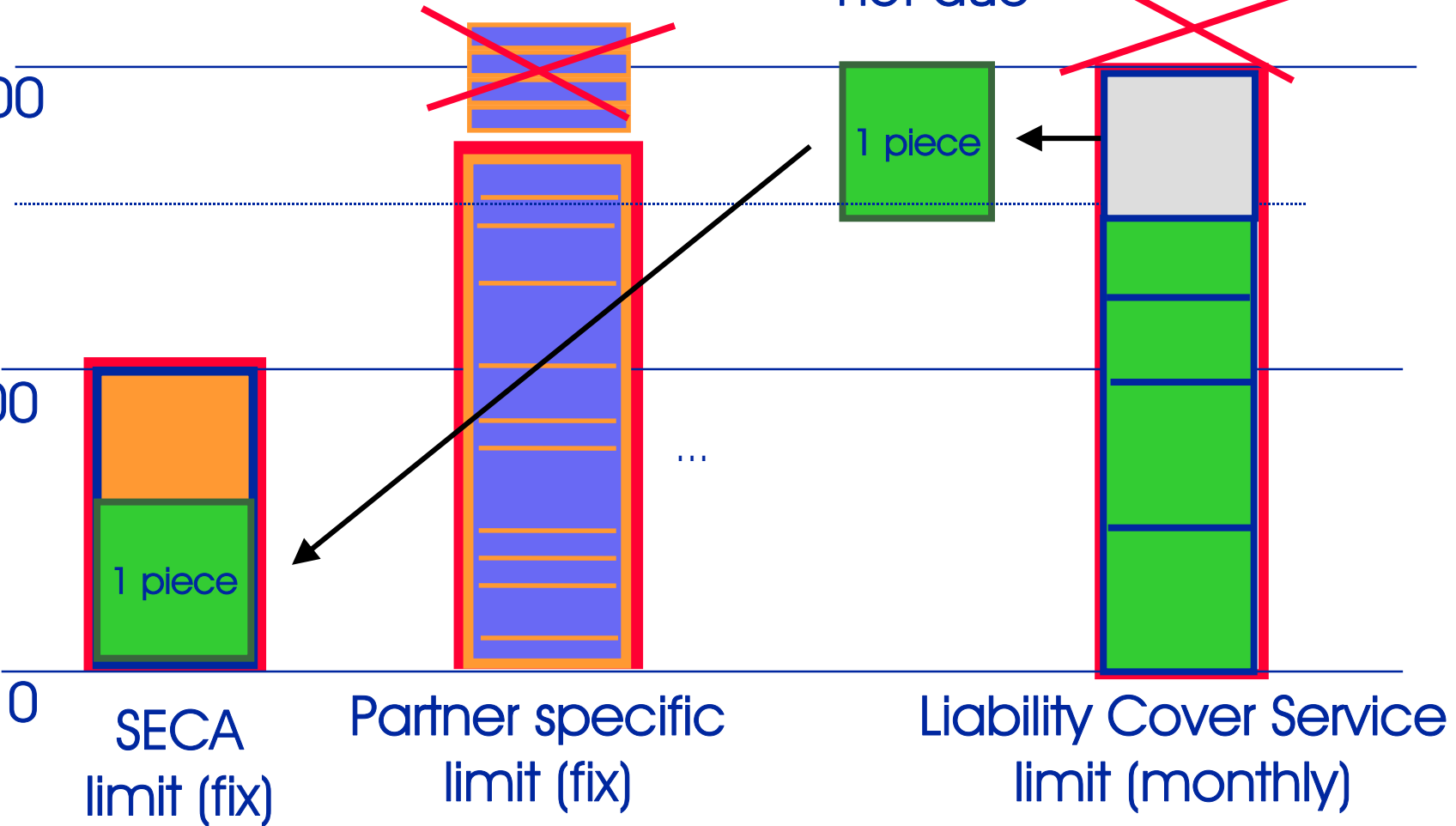
SECA Limit, Partner Specific Limit, Liability Cover Limit

only relevant for compromised signature

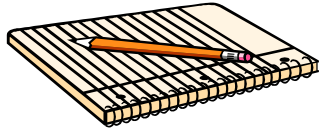guarantee always issued on request, normally not due

Euro 2000

Euro 1000

1 piece

...

1 piece

Euro

0

SECA limit (fix)

Partner specific limit (fix)

Liability Cover Service limit (monthly)
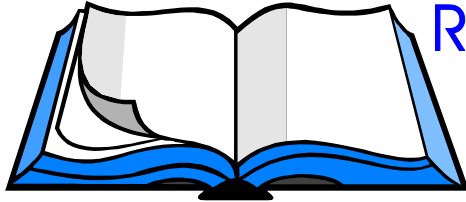
SEMPER

10

'The Code of Conduct'

SECA Defaults

- Applicable Law
- Conclusion of contract
- Personal Data and Confidentiality

Behavior related to Business

- Advertising and Competition
- Negotiation
- Offers and Acceptance
- Consumer Protection Issues
- Content of Contracts and Internet Pages
- Privacy and Data Protection
- Dispute Handling

SEMPER

11

'The Guidelines'

Requirements for 'SECA compliance' of components:

- provide user interface well comprehensive for non technical users
- provide and inform users of means to protect themselves
- prevent attacks
- enforce fair commerce

Recommended user equipment for best protection

Defines equipment levels and shows risks from low
[no secure HW used, any downloaded software used] to high
[secure HW, secure OS used]

'The Guidelines'
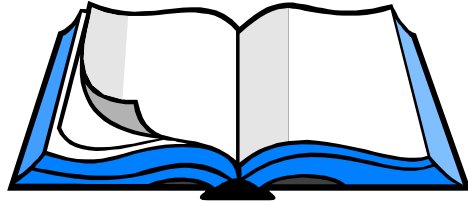
Gives recommendations for best protection

- Care for keys (and access to keys)

- No using any other keys without liability limit

- Care for data

- Use 'SECA compliant' components

- Use a good combination for committed limited liabilities

- Ensure fair commerce

SEMPER

The Benefits of SECA

SECA

§§§§§

signature

- SECA combines essential regulations in one single agreement

- SECA is open for everybody

- SECA protects the key holder from unpredictable damage

- SECA protects the relying party from unpredictable damage

- SECA enforces the awareness of the players

SECA enables fair electronic commerce even for non technical players, NOW!

SEMPER