Limiting Liability in Electronic Commerce:
The Liability Cover Service

Birgit Baum-Waidner
r3 security engineering /
Entrust Technologies Europe
P.O. Box
CH-8301 Glattzentrum/Zürich
Zurich, Switzerland
baum@r3.ch

2nd SEMPER Day
Zurich, Nov 04, 1998

http://www.r3.ch
http://www.entrust.com

Problem: Relying on Transactions

- Can I rely on that Adam will stand by his order?
- Will I suffer damage if he does not?

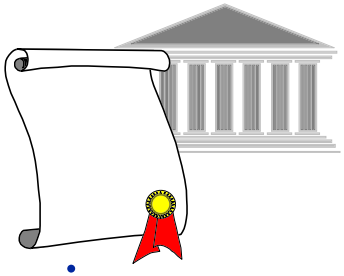
- Will Adam be able to pay?

Adam

Order
Customized PC
à £ 3.500

Retailer
CompBob

Using Public Key Infrastructure



Initially, **CA** identified **Adam**,
certified **Adam's** public key

$sign_{pr\_key\_CA}$ (*pub_key_Adam*, . . .)

- **Can I rely on that Adam will stand by his order?**
- **Will I suffer damage if he does not?**

- **Will Adam be able to pay?**

Adam

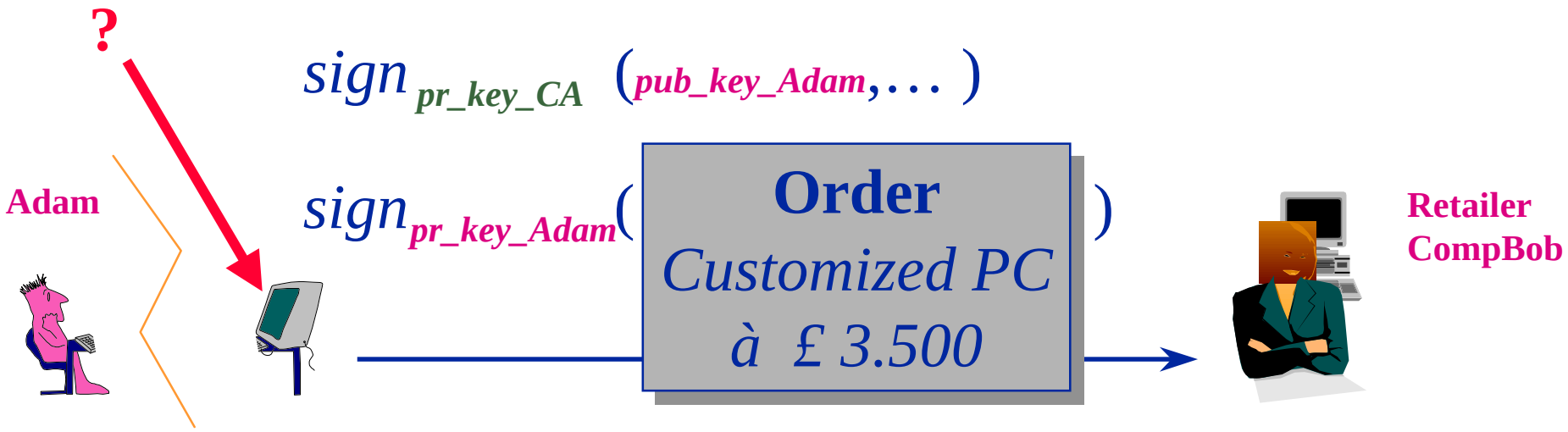
$sign_{pr\_key\_Adam}$ (**Order** *Customized PC à £ 3.500*)

Retailer CompBob

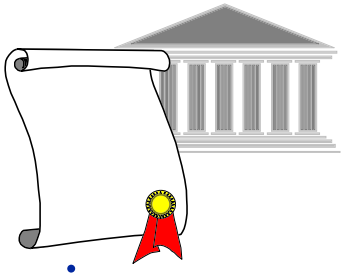
What can go wrong?

Adam's PC creates and signs the order,

but Adam did not authorize it -
at least not ***this order*** to ***this recipient*** with ***this delivery address...***



Assumptions



$sign_{pr\_key\_CA}$ ()

CA is working correctly:
Order was actually signed with ***pr_key_Adam***.

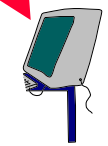
$sign_{pr\_key\_Adam}$( )

Crypto is strong enough, ***pr_key_Adam cannot be broken***

Signature Software, Electronic commerce software are ***completely correct***

?

Adam

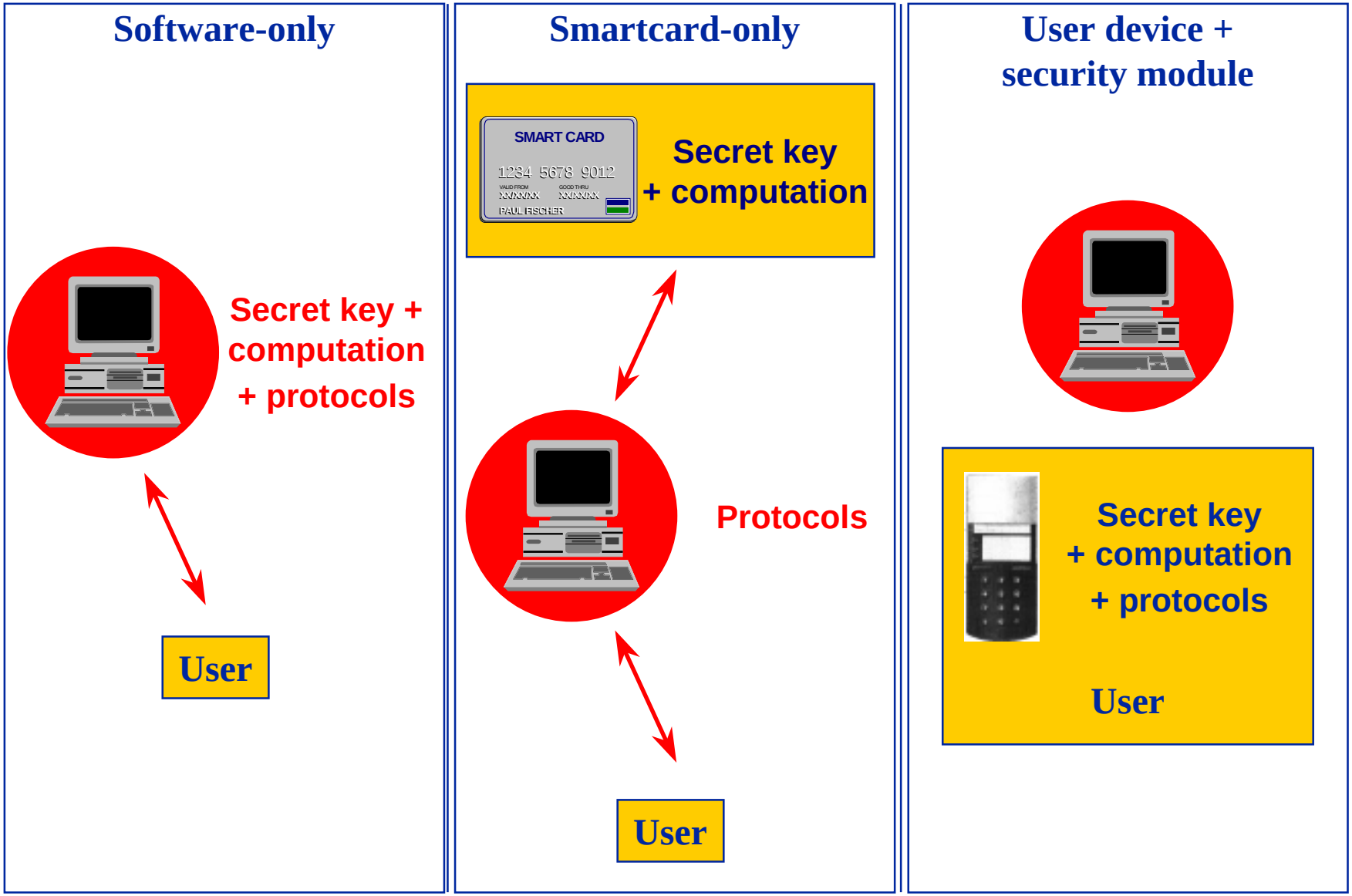


$sign_{pr\_key\_Adam}$(**Order** *Customized PC à £ 3.500*)

Retailer CompBob

SEMPER

Attacks possible through Malicious Software in 'Neighbourhood'



Where are these Threats Relevant?

More relevant

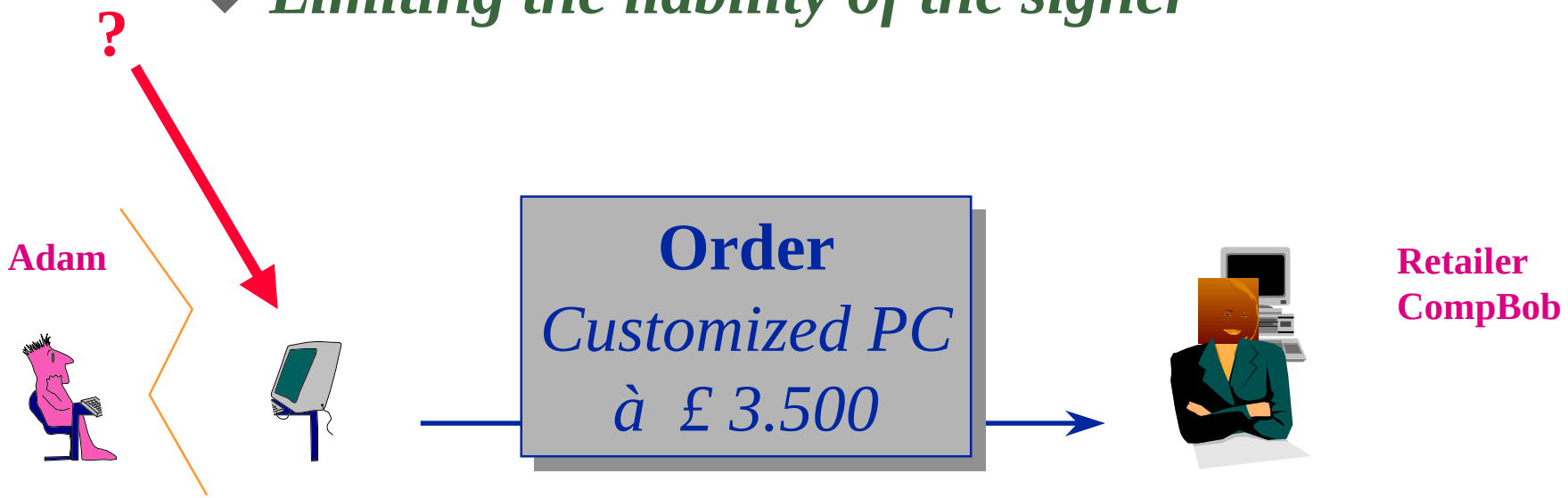
- Well-Established Electronic Commerce Software
  and
- Legal Binding of digital signature with full liability
  and
- Use of signature in open environment, e.g., Internet
  and
- User frequently downloads software from the web
  and
- No secure hardware used

Less relevant

- Application used by few people restricted use
  or
- No legal Binding, or only with liability limit
  or
- Use of signature towards a closed group of recipients
  or
- Use of applications within a closed environment
  or
- Secure Hardware used

Requirements for the Solution

- **Taking into account *impersonating attacks***
- **Use for *non-technical average* Internet user possible**
- **Not forbidding players to *download software***
- ***Non-Deniable Commitment* rather than 'deniable' pre-payment**
- ***Limiting the liability of the signer***



Splitting Signature - Commitment

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

$sign_{pr\_key\_Adam}$(**Order** *Customized PC à £ 3.500* ,)

Adam

Retailer CompBob

SEMPER

Splitting: Signature - Commitment

request

response

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

$sign_{pr\_key\_Adam}$ (**Order** *Customized PC à £ 3.500* ,)

Adam

Retailer CompBob

Splitting: Signature - Commitment

request

response

Non-deniable one-time Commitment

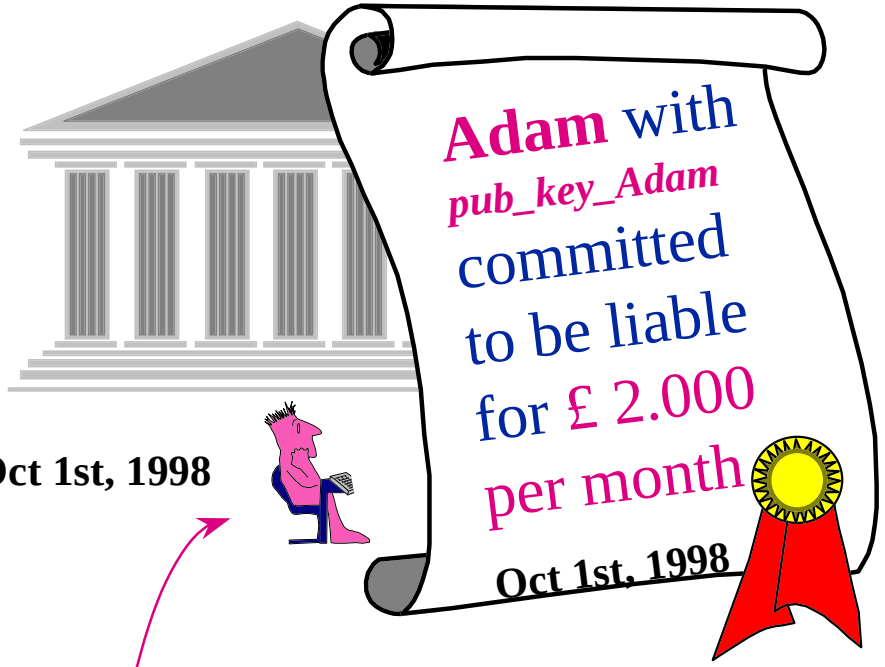
that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

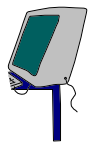
$sign_{pr\_key\_Adam}$ (**Order** *Customized PC à £ 3.500* ,)

Adam

Retailer CompBob

Initialisation





Adam

Retailer
CompBob

Splitting Signature - Commitment

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

$sign_{pr\_key\_Adam}$ (**Order** *Customized PC à £ 3.500* ,)

Adam

Retailer CompBob

Cases

Adam *stands* by his signature	Adam *denies* having made this signature	
Order processed as usual Commitment has no function	Adam claims order invalid, but has to pay *£ 500* .	Adam has actually been attacked
	Adam claims order invalid, but has to pay *£ 500* .	Adam ***lies***

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

Adam

$sign_{pr\_key\_Adam}$ (**Order** *Customized PC à £ 3.500* ,)

Retailer CompBob

Role of Liability Cover Authority

- **Registration** and **Certification Authority** for *pub_key_Adam*
- **Witness** for Adam's commitments
- **Controls limit** of issued commitments
- Confirms that *pub_key_Adam* was **not revoked**
- **Timestamps** Order information

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

$sign_{pr\_key\_Adam}$ (**Order** *Customized PC à £ 3.500* ,)

Adam

Retailer CompBob

Types of Liability Cover Service

Type H (high sensitivity)	*Type N (normal sensitivity)*
◆ LCA has full responsibility and **liability for correct user identification** for 'request'- additional means might be used by the LCA	◆ For identity authentication, LCA has **only to check** Adam's **signature** on the '**request**'
◆ Higher values	◆ Lower values
◆ Higher Liability limit	◆ Lower Liability limit

response

request

Adam

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

SEMPER

Content of LCC Request

Minimum:

- **Adam's LCS Service ID**
- **Adam's ID** (which Adam wants to show to beneficiary)
- **hash**[*)] **(**
  - **unique transaction context ID** of Adam,
  - **a beneficiary's ID** (e.g., fingerprint of his pub_key) **)**
- **amount** (e.g., *£ 500*)
- ***other transaction information***, if any
- **Adam's digital signature**

request

Adam

Content of the Commitment (LCC)

- **Version number of issued certificate**
- **Adam's public key** *pub_key_Adam*
- **Adam's ID** (which Adam wants to show to beneficiary)
- **hash**[*)] **(**
  - **unique transaction context ID** of Adam,
  - **a beneficiary's ID** (e.g., fingerprint of his pub_key) **)**
- **amount** (e.g., *£ 500*)
- ***other transaction information***, if any
- **Date/Time**
- **LCA's signature** and **certificate information**

response

Adam

Anonymity

Anonymity can be achieved:

- Signer towards relying party
  by pseudonyms

Retailer
CompBob

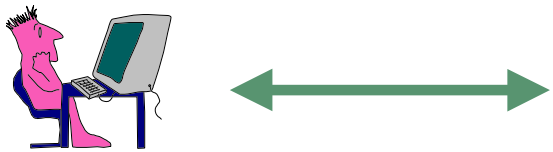
PSAdam

Who sent the order???

- Relying party and transaction towards Authority
  by hashing transaction information is hashed.

?

What kind of business is Adam doing?
With whom?



Commitment Service

- **General Service**, it includes LCS as special case
- **Any possible validity condition** can be specified by Adam (on initialization, or in the ‘request’), e.g.,
  - **“If I withdraw this order”**
  - **“on your birthday”**
  - **“if you give me X in exchange”**
  - **“unconditionally”**
- **Any commitments possible:** Commitment Authority controls a **set of Commitments** (per month), also such like **“10 hours piano tuning”**

Liability Cover Service

- **Special Service Type** of Commitment Service
- **Fixed validity condition:**
  - **“If the signature is claimed compromized”**
- Only **commitments over amounts of money:** LCA controls an **amount of money** (per month), e.g., £ 2.000

Problem: Relying on Transactions

- **Can I rely on that Adam will stand by his order?** ***No.***
- **Will I suffer damage if he does not?** ***No.***

- **Will Adam be able to pay?**

If LCS is performed **by a bank,**
it can be used as a **combined**
Liability Cover Service
and
‘Solvency Service’

Retailer
CompBob

Fit in Legal Framework

Separation between:

Order *Customized PC* *à £ 3.500*	**Non-deniable one-time Commitment** that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**
Signature	**Undeniable Commitment**

enables **Agreements** regulating scope, validity and liability limit of signatures

Validity and Scope of Signature can be restricted to

- validity only within the **conditions specified in an agreement** (e.g., ***SEMPER Electronic Commerce Agreement***)
- validity only if **not denied**

An **Undeniable Commitment** might satisfy the relying party, if signature is denied

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

SEMPER

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

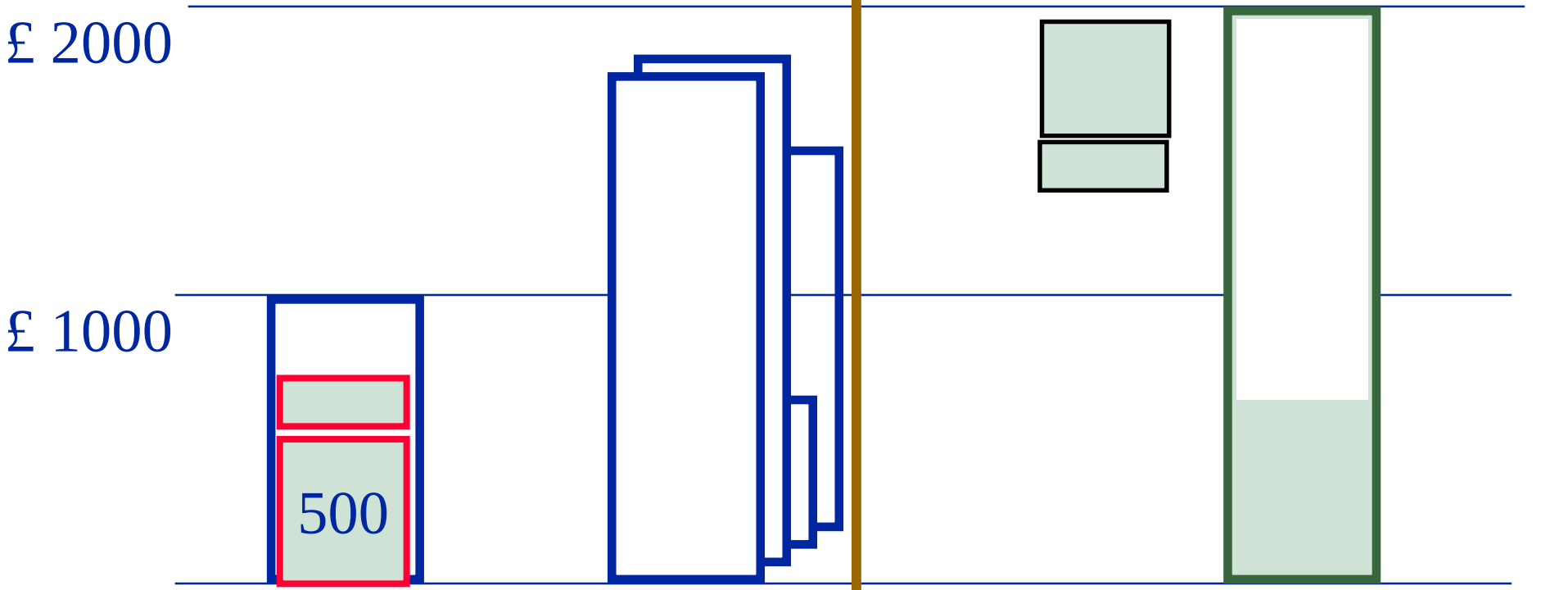
Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due



General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

SEMPER

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

500

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 0

3000

500

Unspecific limit (fix)

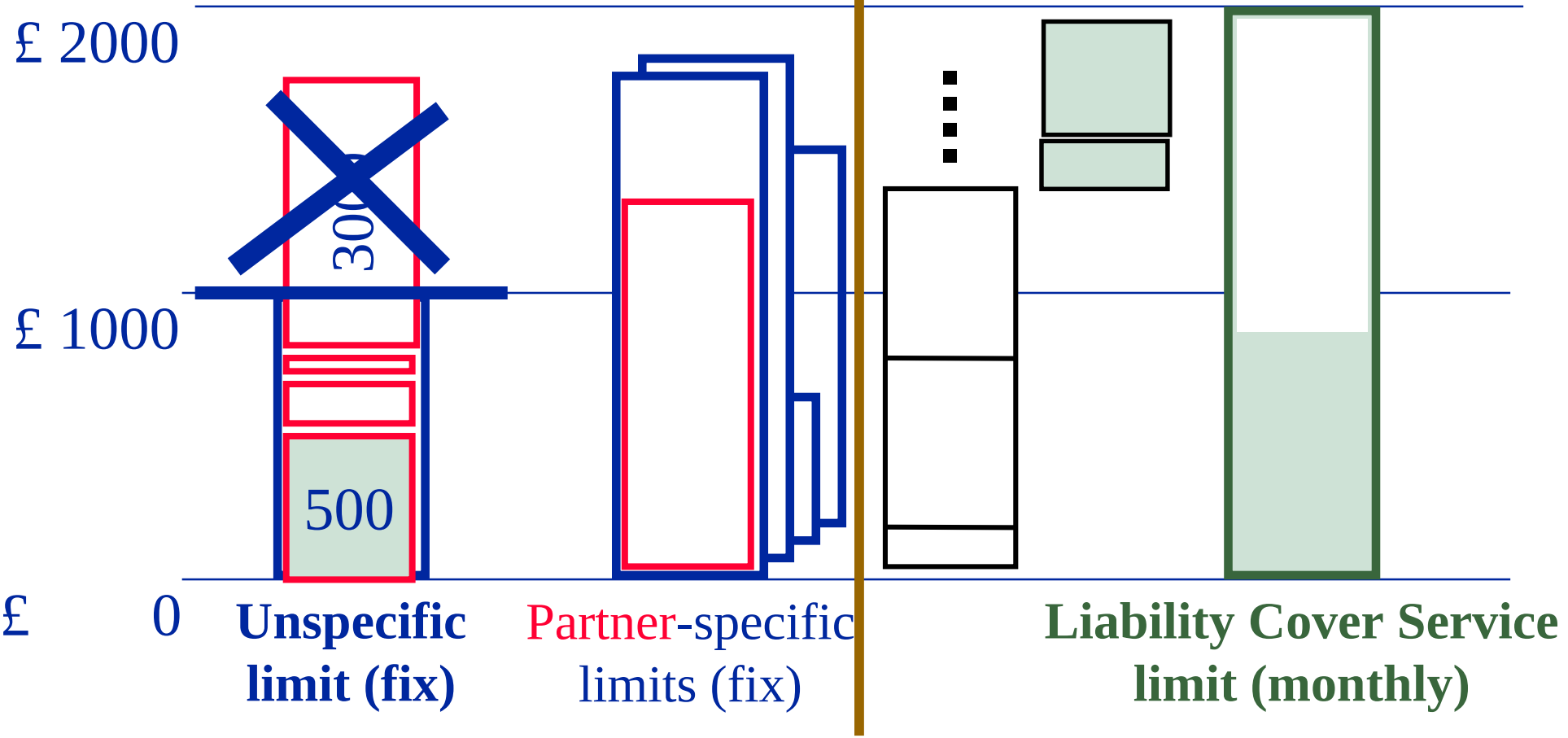
Partner-specific limits (fix)

Liability Cover Service limit (monthly)

General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due



Benefits of Commitment Service

- Enables **Separation**

Order
Customized PC
à £ 3.500

Signature

Non-deniable one-time Commitment

that **Adam** is liable for *£ 500* in case that he denies the signature for **this Order**

Undeniable Commitment

- Protects **Relying party** by **enabling undeniable commitments**
- Protects **Signer** by **limiting the issued commitments** in the compromized case, also in case of **Advanced Attacks** which **might not be able to be proven**
- Is the **only existing Multiparty Security solution** for **Open Electronic Commerce** and digital signatures to be performed by the **average non-technical Internet user**, with insecure equipment and using downloaded software