Limiting Liability in Electronic Commerce:  
The Liability Cover Service  

2nd SEMPER Day  
Zurich, Nov 04, 1998
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?

Order
Customized PC à £ 3,500
Using Public Key Infrastructure

Initially, CA identified Adam, certified Adam’s public key

\[ \text{sign}_{pr\_key\_CA} \left( pub\_key\_Adam, \ldots \right) \]

- 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?

Order Customized PC à £ 3.500
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

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

Crypto is strong enough, pr_key_Adam cannot be broken.

Signature Software, Electronic commerce software are completely correct.

Order
Customized PC
à £ 3,500
Attacks possible through Malicious Software in ‘Neighbourhood’

Software-only

Secret key + computation + protocols

User

Smartcard-only

Secret key + computation

Protocols

User

User device + security module

Secret key + computation + protocols

User
## Where are these Threats Relevant?

<table>
<thead>
<tr>
<th>More relevant</th>
<th>Less relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>◆ Well-Established Electronic Commerce Software and</td>
<td>◆ Application used by few people restricted use or</td>
</tr>
<tr>
<td>◆ Legal Binding of digital signature with full liability and</td>
<td>◆ No legal Binding, or only with liability limit or</td>
</tr>
<tr>
<td>◆ Use of signature in open environment, e.g., Internet and</td>
<td>◆ Use of signature towards a closed group of recipients or</td>
</tr>
<tr>
<td>◆ User frequently downloads software from the web and</td>
<td>◆ Use of applications within a closed environment or</td>
</tr>
<tr>
<td>◆ No secure hardware used</td>
<td>◆ Secure Hardware used</td>
</tr>
</tbody>
</table>
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**

\[
sign_{pr \_key \_Adam}(\text{Order Customized PC à £ 3.500})
\]
Splitting: Signature - Commitment

Non-deniable one-time Commitment that **Adam** is liable for **£ 500** in case that he denies the signature for **this Order**.

**Order**

Customized PC

à  £ 3.500

*sign*_{pr_key_Adam} (  ,  )
Splitting: Signature - Commitment

Adam with \textit{pub\_key\_Adam} committed to be liable for £ 2.000 per month

\textbf{Non-deniable one-time Commitment} that Adam is liable for £ 500 in case that he denies the signature for \textbf{this Order}.

\textbf{Order}:
\begin{itemize}
  \item Customized PC
  \item à £ 3.500
\end{itemize}

\textbf{Retailer CompBob}
Initialisation

Adam with pub_key_Adam committed to be liable for £2,000 per month from Oct 1st, 1998.

Oct 1st, 1998
Splitting Signature - Commitment

Adam with 
\( \text{pub}_\text{key}_\text{Adam} \)
committed 
to be liable 
for £ 2,000 
per month

Oct 1st, 1998

Non-deniable one-time Commitment 
that Adam is liable for £ 500 in case that he denies the signature for this Order

\[ \text{sign}_{\text{pr}_\text{key}_\text{Adam}}(\text{Order Customized PC à £ 3,500} , \text{Retailer CompBob}) \]
Cases

Adam *stands* by his signature

Order processed as usual
Commitment has no function

Adam *denies* having made this signature

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

\[
\text{sign}_{pr\_key\_Adam}(\text{Order Customized PC à £ 3.500}),
\]

Retailer CompBob

Adam

sign_{pr_key_Adam}(\text{Order Customized PC à £ 3.500}),

Retailer CompBob

Adam

Adam

Adam
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, ( ) )
```
Types of Liability Cover Service

**Type H (high sensitivity)**
- LCA has full responsibility and **liability for correct user identification** for ‘request’- additional means might be used by the LCA
- Higher values
- Higher Liability limit

**Type N (normal sensitivity)**
- For identity authentication, LCA has **only to check** Adam’s **signature** on the ‘request’
- Lower values
- Lower Liability limit

---

Non-deniable one-time Commitment
that Adam is liable for **£ 500** in case that he denies the signature for **this Order**
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
**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
Anonymity can be achieved:

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

Who sent the order???

What kind of business is Adam doing?

With whom?
<table>
<thead>
<tr>
<th>Commitment Service</th>
<th>Liability Cover Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Service</strong>, it includes LCS as special case</td>
<td><strong>Special Service Type</strong> of Commitment Service</td>
</tr>
<tr>
<td><strong>Any possible validity condition</strong> can be specified by Adam (on initialization, or in the ‘request’), e.g.,</td>
<td><strong>Fixed validity condition:</strong></td>
</tr>
<tr>
<td>◆ “If I withdraw this order”</td>
<td>◆ “If the signature is claimed compromized”</td>
</tr>
<tr>
<td>◆ “on your birthday”</td>
<td></td>
</tr>
<tr>
<td>◆ “if you give me X in exchange”</td>
<td></td>
</tr>
<tr>
<td>◆ “unconditionally”</td>
<td></td>
</tr>
<tr>
<td><strong>Any commitments possible</strong>: Commitment Authority controls a set of Commitments (per month), also such like <strong>10 hours piano tuning</strong></td>
<td><strong>Only commitments over amounts of money</strong>: LCA controls an amount of money (per month), e.g., £ 2.000</td>
</tr>
</tbody>
</table>
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.

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

Separation between:

Order
Customized PC
à £ 3.500

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

Non-deniable one-time Commitment that Adam is liable for £ 500 in case that he denies the signature for this Order

Order
Customized PC
à £ 3.500

Valid only if not denied.
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**
  - £ 1000
  - £ 2000

- **Partner-specific limits (fix)**
  - Commitment always issued on request, normally not due

- **Liability Cover Service limit (monthly)**
  - Only relevant for compromised signature
  - Commitment always issued on request, normally not due
General Limit, Partner specific Limit, Liability Cover Limit

- Unspecific limit (fix)
- Partner-specific limits (fix)
- Liability Cover Service limit (monthly)

Commitment always issued on request, normally not due.

Only relevant for compromised signature.
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

<table>
<thead>
<tr>
<th>£ 2000</th>
<th>£ 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>£ 2000</td>
<td>£ 1000</td>
</tr>
</tbody>
</table>

- Unspecific limit (fix)
- Partner-specific limits (fix)
- Liability Cover Service limit (monthly)

- Only relevant for compromised signature
- Commitment always issued on request, normally not due
General Limit, Partner specific Limit, Liability Cover Limit

**Unspecific limit (fix)**
- £ 1000

**Partner-specific limits (fix)**
- £ 2000

**Liability Cover Service limit (monthly)**
- £ 500

*commitment always issued on request, normally not due*

*only relevant for compromised signature*
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £2000
- **Partner-specific limits (fix)**: £1000
- **Liability Cover Service limit (monthly)**: £500

Commitment always issued on request, normally not due.

Only relevant for compromised signature.
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £500
- **Partner-specific limits (fix)**: £1000
- **Liability Cover limit (monthly)**: £2000

**Notes:**
- Only relevant for compromised signature.
- Commitment always issued on request, normally not due.
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £ 500
- **Partner-specific limits (fix)**: £ 1000
- **Liability Cover limit (monthly)**: £ 2000

Only relevant for compromised signature.

Commitment always issued on request, normally not due.
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £1000
- **Partner-specific limits (fix)**: £500
- **Liability Cover Service limit (monthly)**: £1000

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 500

£ 0
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: €1000
- **Partner-specific limits (fix)**: €2000
- **Liability Cover Service limit (monthly)**: Unspecified

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

£ 500

£ 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
- Unspecific limit (fix)
  - £ 1000
  - 500

Partner-specific limits (fix)
- £ 1000
- £ 2000

Liability Cover Service limit (monthly)
- £ 500
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £1000
- **Partner-specific limits (fix)**: £2000
- **Liability Cover Service limit (monthly)**: £500

Commitment always issued on request, normally not due.

- Only relevant for compromised signature.
General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £1000 to £2000
- **Partner-specific limits (fix)**: £500
- **Liability Cover Service limit (monthly)**: Commitment always issued on request, normally not due

only relevant for compromised signature
General Limit, Partner specific Limit, Liability Cover Limit

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

<table>
<thead>
<tr>
<th>£ 2000</th>
<th></th>
<th>£ 1000</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unspecific limit (fix)</td>
<td></td>
<td>Liability Cover Service limit (monthly)</td>
</tr>
<tr>
<td></td>
<td>Partner-specific limits (fix)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>£</td>
<td>0</td>
<td>£</td>
<td></td>
</tr>
</tbody>
</table>

- General Limit
- Partner-specific Limit
- Liability Cover Limit
- 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

- Unspecific limit (fix)
- Partner-specific limits (fix)
- Liability Cover Service limit (monthly)
General Limit, Partner specific Limit, Liability Cover Limit

- Unspecific limit (fix)
- Partner-specific limits (fix)
- Liability Cover Service limit (monthly)

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

Unspecific limit (fix)  Partner-specific limits (fix)  Liability Cover Service limit (monthly)

£ 1000

£ 2000

500
General Limit, Partner specific Limit, Liability Cover Limit

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

- £ 2000
  - Unspecific limit (fix)
  - Partner-specific limits (fix)
  - Liability Cover Service limit (monthly)

- £ 1000
  - Unspecific limit (fix)

- £ 500

- £ 0
General Limit, Partner specific Limit, Liability Cover Limit

only relevant for compromised signature

commitment always issued on request, normally not due

£ 2000

£ 1000

£ 500

£

0

Unspecific limit (fix)

Partner-specific limits (fix)

Liability Cover Service limit (monthly)
General Limit, Partner specific Limit, Liability Cover Limit

- Unspecific limit (fix): £1000
- Partner-specific limits (fix): £2000
- Liability Cover Service limit (monthly): £500

only relevant for compromised signature

commitment always issued on request, normally not due
General Limit, Partner specific Limit, Liability Cover Limit

- General Limit
  - Partner specific Limit
- Liability Cover Limit

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

£ 2000
- Unspecific limit (fix) £ 1000
- Partner-specific limits (fix) £ 2000
- Liability Cover Service limit (monthly) £ 500

£ 1000
- Unspecific limit (fix) £ 500
- Partner-specific limits (fix) £ 2000
- Liability Cover Service limit (monthly) £ 1000

£ 0
General Limit, Partner specific Limit, Liability Cover Limit

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

<table>
<thead>
<tr>
<th>£ 2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecific limit (fix)</td>
</tr>
<tr>
<td>Partner-specific limits (fix)</td>
</tr>
<tr>
<td>Liability Cover Service limit (monthly)</td>
</tr>
</tbody>
</table>

- £ 500
- £ 2000
- £ 1000
General Limit, Partner specific Limit, Liability Cover Limit

- Unspecified limit (fix)
  - £ 2000
- Partner-specific limits (fix)
  - £ 2000
- Liability Cover Service limit (monthly)
  - £ 1000

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

- £ 500

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

- £ 500

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

- £ 500

- Only relevant for compromised signature
- Commitment always issued on request, normally not due

- £ 500
General Limit, Partner specific Limit, Liability Cover Limit

- only relevant for compromised signature
- commitment always issued on request, normally not due

£ 2000
- Unspecific limit (fix): £3000
- Partner-specific limits (fix): £500

£ 1000
- Liability Cover Service limit (monthly): £500

£
- 0
- Unspecific limit (fix)
- Partner-specific limits (fix)
- Liability Cover Service limit (monthly)
### General Limit, Partner specific Limit, Liability Cover Limit

- **Unspecific limit (fix)**: £500
- **Partner-specific limits (fix)**: £2000
- **Liability Cover Service limit (monthly)**: £1000

**Note:** Only relevant for compromised signature. Commitment always issued on request, normally not due.
Benefits of Commitment Service

- Enables Separation

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customized PC</td>
</tr>
<tr>
<td>€ 3,500</td>
</tr>
</tbody>
</table>

Signature

Undeniable Commitment

- Protects Relying party by enabling undeniable commitments

- Protects Signer by limiting the issued commitments in the compromised 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