# P3P - Platform for Privacy Preferences

**Sicherheit/Vertrauen**

DB-Aspekte des E-Commerce, Schwerpunkt: Techniken

Johannes Herlitz <j_herlit@informatik.uni-kl.de>

# Gliederung

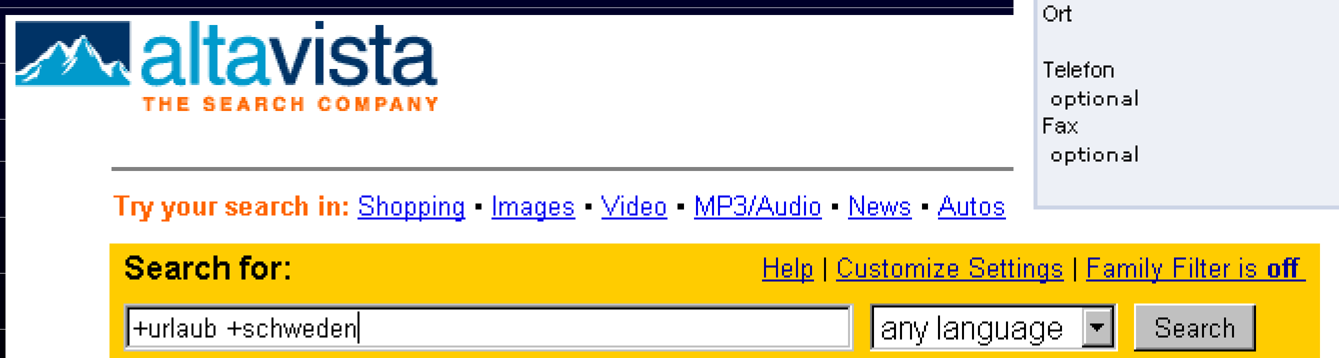
1. Motivation und Problem
2. Lösungsansätze
3. P3P - Überblick
4. P3P - Sprachelemente
5. Ausblick

# Motivation (1)

Preisgabe von persönlicher Information

- explizit


- implizit



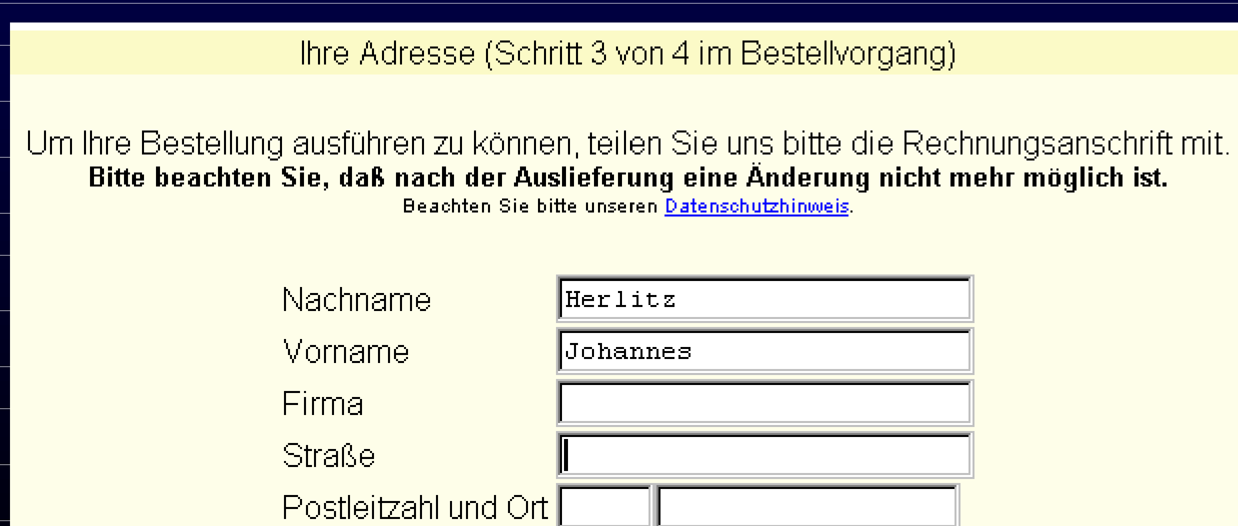
# Motivation (2)

Hilfe: *Anonymizer.com* teilweise gegen implizite Informationssammlung (IP, Browsertyp,... )

⇒ Vertrauen gegenüber *Anonymizer.com*

# Motivation (3)

- *Anonymizer.com*: kein Schutz bei Formularen
- keine Kontrolle über Benutzung meiner persönlichen Daten


Ihre Adresse (Schritt 3 von 4 im Bestellvorgang)

Um Ihre Bestellung ausführen zu können, teilen Sie uns bitte die Rechnungsanschrift mit.
**Bitte beachten Sie, daß nach der Auslieferung eine Änderung nicht mehr möglich ist.**
Beachten Sie bitte unseren Datenschutzhinweis.

| | |
|---|---|
| Nachname | Herlitz |
| Vorname | Johannes |
| Firma | |
| Straße | |
| Postleitzahl und Ort | |

# Problematik

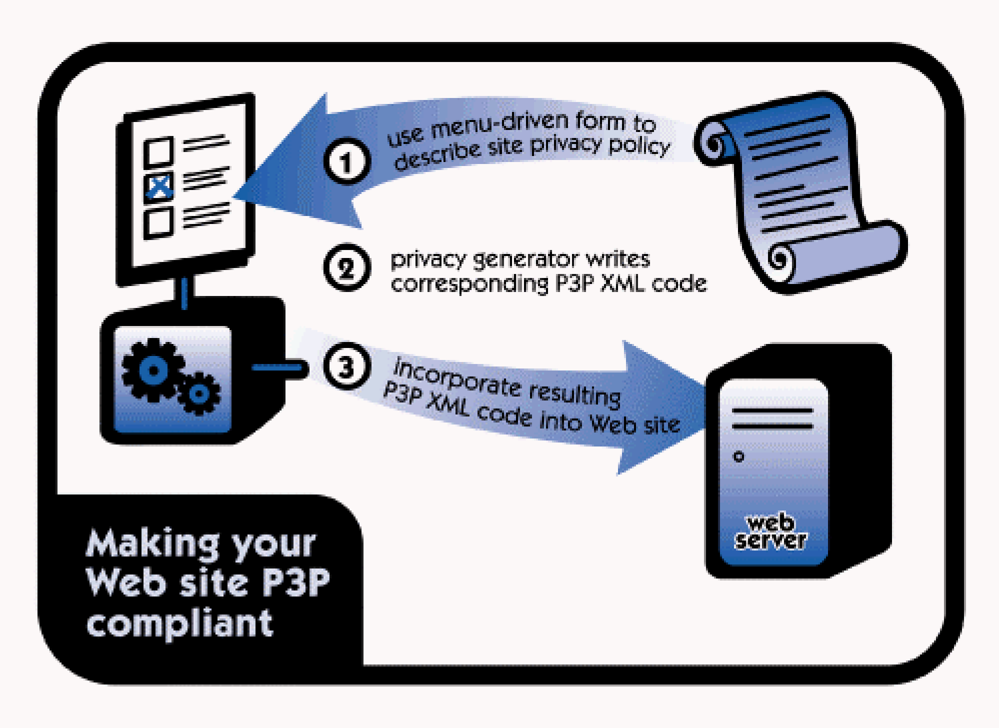
- keine Möglichkeit, anzugeben, was mit meinen Daten passiert
- keine Kontrolle über meine Daten
- wünschenswert: automatisches Ausfüllen von Formularen
- Problem: jede Web-Site kann sich meine Adresse besorgen

# Überblick: P3P

- Überwacht, ***wer wozu was*** sammelt und evtl. an ***wen was*** weitergegeben wird.
  - Clickstreams, Postaddresse, E-Mail,...
  - Aktuelle Transaktion, Kundenstudien, ...
  - Weitergabe von E-Mail für Werbezwecke
- basiert auf XML
- setzt auf HTTP auf

# serverseitige Vorbereitung (1)

- Policy-Generatoren helfen bei der Erzeugung von P3P-Policies



# serverseitige Vorbereitung (2)

- policy reference file **/w3c/p3p.xml**

```
<?xml version="1.0" encoding="UTF-8" ?>
<meta xmlns="http://www.w3.org/2000/12/P3Pv1">
 <POLICY-REFERENCES>
  <POLICY-REF about="/p3p/Policy1.xml">
   <INCLUDE>/*</INCLUDE>
  </POLICY-REF>
 </POLICY-REFERENCES>
</meta>
```

- policy file

**/p3p/Policy1.xml**

```
<POLICY xmlns="http://www.w3.org/2000/12/P3Pv1“
   discuri="http://www.katalog.beispiel.de/index.html">
  <ENTITY>
    <DATA-GROUP>
      <DATA ref="#business.name">Beispielfirma</DATA>
      <DATA ref="#business.contact-info.postal.street">Hauptstrasse 123</DATA>
      <DATA ref="#business.contact-info.postal.city">Kaiserslautern</DATA>
      <DATA ref="#business.contact-info.postal.country">Germany</DATA>
...
```

# serverseitige Vorbereitung (3)

- Einbinden in WWW Server
- Selbstgeschriebenes oder generiertes „policy reference file“ und alle „policy files“ auf dem Webserver ablegen

**/home/www/documents/**

```
/w3c/p3p.xml

/<pfad>/Policy1.xml
/<pfad>/Policy2.xml
/<pfad>/Policy3.xml
```

# Finden von policy reference files

## 3 Möglichkeiten

**well-known location**

```
/w3c/p3p.xml
```

**HTML <link> tag:**

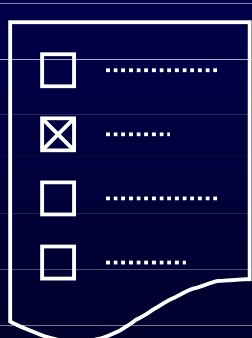
```
<link rel="P3Pv1"
href="http://foo...">
```

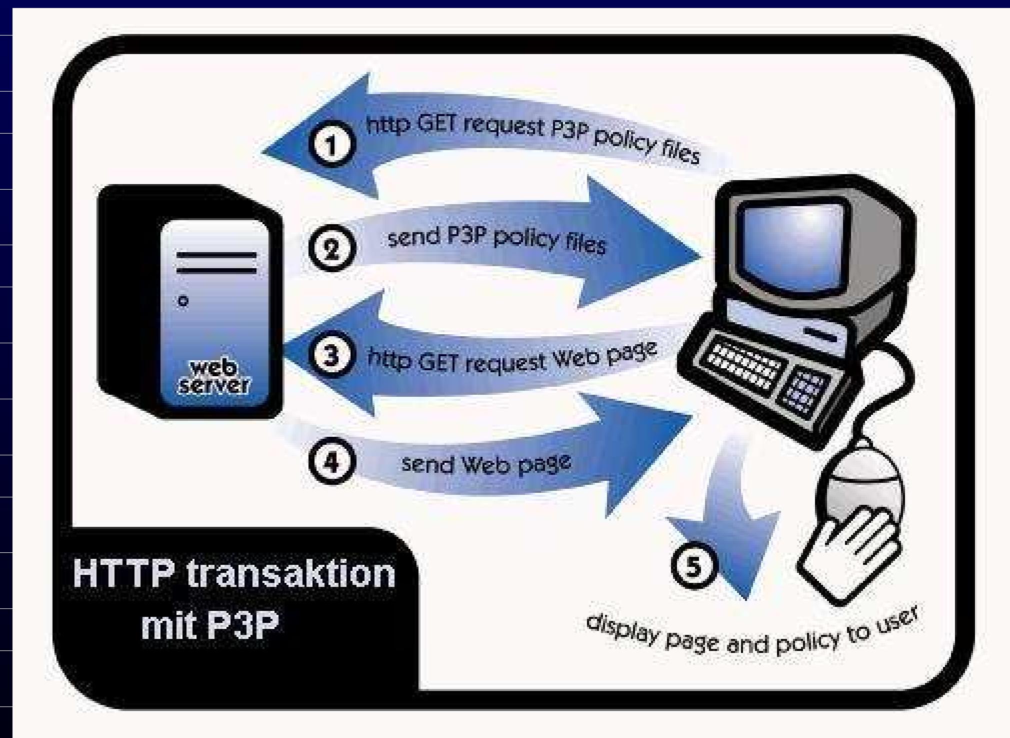
**HTTP headers:**

```
$ telnet localhost 80
...

HTTP/1.1 200 OK
Date: Sun, 10 Jun 2001 20:53:19 GMT
Server: Apache/1.3.19 (Unix)  (SuSE/Linux) PHP/4.0.4pl1
P3P: policyref="http://foo.bar/w3c/p3p.xml"
Content-Length: 534
Content-Type: text/html

<html>
<head>
  <title>Welcome to http://foo.bar</title>
</head>
...
```

# Clientseite (1)

- Kunden nutzen Browser mit P3P Unterstützung
- P3P konfigurieren



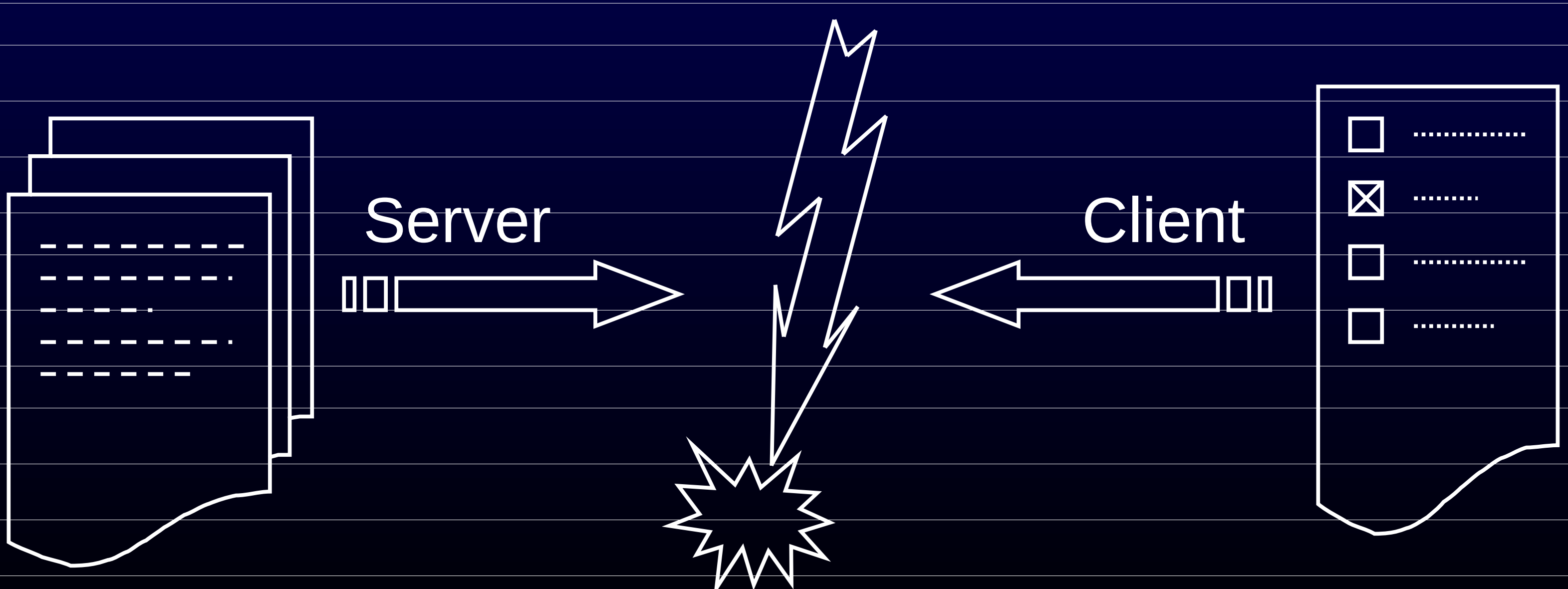


# Clientseite (2)

- Policy reference file **finden**
- Policy reference file **holen**
- Policy reference file **parsen**
- Alle benötigten P3P policies **holen**
- Alle geholten P3P policies **parsen**

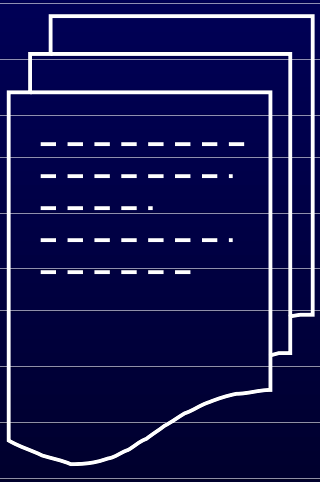
# Konfliktfall

- bei Konflikt von geholter Policy und persönlichen Einstellungen wird eine Warnung ausgegeben, z.B. ein Popup



# P3P Policy

- P3P policy file
  - **ENTITY**
  - **DISPUTES-GROUP**
    - **REMEDIES**
  - **STATEMENT**
    - **PURPOSE**
    - **RECIPIENT**
    - **RETENTION**
    - **DATA-GROUP**
      - **DATA**



- Site-interne vs. Site-externe Aspekte

# Fähigkeiten von P3P

- Site-extern
  - ***Wer*** sammelt meine Daten ?
  - ***Was*** genau wird gesammelt ?
  - **W*arum*** wird meine Information gebraucht ?
  - Welcher Teil wird ***weitergegeben*** ?
  - ***An wen*** wird der Teil weitergegeben ?

# ***Wer*** sammelt meine Daten ?


```
<ENTITY>
  <DATA-GROUP>
    <DATA ref="#business.name">Beispielkatalog</DATA>
    <DATA ref="#business.contact-info.postal.street">Hauptstrasse 234</DATA>
    <DATA ref="#business.contact-info.postal.city">Kaiserslautern</DATA>
    <DATA ref="#business.contact-info.postal.stateprov">RP</DATA>
    <DATA ref="#business.contact-info.postal.postalcode">67663</DATA>
    <DATA ref="#business.contact-info.postal.country">Germany</DATA>
    <DATA ref="#business.contact-info.online.email">info@beispiel.de</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.intcode">49</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.loccode">631</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.number">123456</DATA>
  </DATA-GROUP>
</ENTITY>
```

# ***Was*** wird gesammelt ? (1)

```
<STATEMENT>
  <CONSEQUENCE>
    We record some information in order to serve your request
    and to secure and improve our Web site.
  </CONSEQUENCE>
  <PURPOSE><admin/><develop/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#dynamic.clickstream.server"/>
    <DATA ref="#dynamic.http.useragent"/>
  </DATA-GROUP>
</STATEMENT>
```

# *Was* wird gesammelt ? (2)

```
<STATEMENT>
  <CONSEQUENCE>
    We use this information when you make a purchase.
  </CONSEQUENCE>
  <PURPOSE><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.postal"/>
    <DATA ref="#user.home-info.telecom.telephone"/>
    <DATA ref="#user.business-info.postal"/>
    <DATA ref="#user.business-info.telecom.telephone"/>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><purchase/></CATEGORIES>
    </DATA>
  </DATA-GROUP>
</STATEMENT>
```

# ***Warum*** werden Informationen benötigt ?

```
<STATEMENT>
  <CONSEQUENCE>
    We use this information when you make a purchase.
  </CONSEQUENCE>
  <PURPOSE><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.postal"/>
    <DATA ref="#user.home-info.telecom.telephone"/>
    <DATA ref="#user.business-info.postal"/>
    <DATA ref="#user.business-info.telecom.telephone"/>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><purchase/></CATEGORIES>
    </DATA>
  </DATA-GROUP>
</STATEMENT>
```

# Werte von `<PURPOSE>`

– **`<current/>`**
– **`<admin/>`**
– **`<develop/>`**
– Personalisierung **`(customization, tailoring, pseudo-analysis, pseudo-decision, individual-analysis, individual-decision)`**
– Kontaktinformationen **`(contact, telemarketing)`**
– Benutzerdefniniert **`(other-purpose)`**

# ***Weitergabe*** von Informationen

```
<STATEMENT>
  <CONSEQUENCE>
    We use this information when you make a purchase.
  </CONSEQUENCE>
  <PURPOSE><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.postal"/>
    <DATA ref="#user.home-info.telecom.telephone"/>
    <DATA ref="#user.business-info.postal"/>
    <DATA ref="#user.business-info.telecom.telephone"/>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><purchase/></CATEGORIES>
    </DATA>
  </DATA-GROUP>
</STATEMENT>
```

# Werte von <RECIPIENT>

- <ours/>
- <same/>
- <other-recipient/>
- <delivery/>
- <public/>
- <unrelated/>

# Fähigkeiten von P3P

Site-intern

- ***Änderung*** meiner Information möglich ?
- Wie werden ***Verstöße*** *gelöst* ?
- Wie ist die Vorgehensweise bei der ***Speicherung*** meiner Daten ?
- Wo kann ich ***Details*** in verständlicher Form nachlesen ?

# Verstöße

- Folgen und Schadensersatz

```
<DISPUTES-GROUP>
  <DISPUTES resolution-type="independent"
    service="http://www.PrivacySeal.example.org"
    short-description="PrivacySeal.example.org">
    <IMG src="http://www.PrivacySeal.example.org/Logo.gif" alt="logo"/>
    <REMEDIES><correct/></REMEDIES>
  </DISPUTES>
</DISPUTES-GROUP>
```

- weitere Werte:

```
<REMEDIES><money/><law/></REMEDIES>
```

# Kurzbeschreibung einer Policy

```
<STATEMENT>
  <CONSEQUENCE>
    We use this information when you make a purchase.
  </CONSEQUENCE>
  <PURPOSE><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.postal"/>
    <DATA ref="#user.home-info.telecom.telephone"/>
    <DATA ref="#user.business-info.postal"/>
    <DATA ref="#user.business-info.telecom.telephone"/>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><purchase/></CATEGORIES>
    </DATA>
  </DATA-GROUP>
</STATEMENT>
```

# Cookies

- policy reference file

```
<META xmlns="http://www.w3.org/2000/12/P3Pv1">
  <POLICY-REFERENCES>
    <POLICY-REF about="/p3p/Policy1.xml">
      <INCLUDE>/*</INCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
</META>
```

```
<META xmlns="http://www.w3.org/2000/12/P3Pv1">
  <POLICY-REFERENCES>
    <POLICY-REF about="/P3P/CookiePolicy1.xml">
      <COOKIE-INCLUDE>* * *</COOKIE-INCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
</META>
```

# Zusammenfassung

- Server leicht P3P-aktivierbar
- Implementierung von P3P in Clients nötig
- es entsteht eine Sensibilisierung beim Surfen
- P3P als technische Seite jetzt vorhanden, Juristen können darauf aufbauen

# Ausblick

- P3P bietet keine Garantie für die Einhaltung der Policies vom Anbieter
- weltweite Gesetzgebung und Strafverfolgung fehlt
- entsprechende Paragraphen in Deutschland allein sind ein Anfang
- P3P Unterstützung von Clients fehlt, vor allem bei den verbreiteten Browser (IE und NS)