

Rechtsicherheit im elektronischen Geschäftsverkehr

Der „IST“ – Zustand

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Benötigt wird**
 - revisionssichere Korrespondenz
- **Umsetzung durch**
 - (kryptographische, monovalente) elektronische Signatur
- **zu beachten sind**
 - Protokolle, Verhaltensvorschriften
- **Fazit**
 - zu kompliziert, zu anfällig, nicht praxistauglich

Grundsätzliche Anforderungen

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Vertraulichkeit**
 - **Integrität**
- **Zurechenbarkeit**
 - **Verfügbarkeit**

Bundesamt für Sicherheit in Informationstechnik

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

Department of Defence

(US-Verteidigungsministerium):

a trusted system is one,
which **can** break the security policy

Ein System des Vertrauens ist **im Stande** Grundsätze
der Sicherheit zu brechen.

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Europäische Kommission (Nov. 2004)**
 - offene, frei zugängliche Standards (niemanden ausschließen!)
- **JKomG (Nov. 2004)**
 - Unicode, ASCII, XML, TIFF, ZIP
- **UStG §14** Echtheit der Herkunft und die Unversehrtheit des Inhalts gewährleisten durch 1. SigG oder 2. ... kompliziert
- **SigG**

elektronische Unterschrift

Exkurs



elektronische Unterschrift

Exkurs



Zertifizierer

§11 SigG: schuldhafte Pflicht- & Produkthaftung

§12 ≤ 250.000 € je Fall *geeignete Deckungsvorsorge*

Notare

§ 19 BNotO: persönlich, unbeschränkbare Haftung

§ 19a(3): ≥ 500.000 € je Fall, ≥ 2 x pro Jahr versichert

- **Wie versichern?**

Vorsatz – Pishing – Fortschritt

- **Wenige Zertifizierer – viele Kunden**

- hoher Wert im Schlüssel

- oft gebraucht

- leicht korrumpierbar

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

Logische Zuordnung sei

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

nicht korrumpierbar (nicht manipulierbar)

Kein Individuum kann ein anderes verkörpern.

störfest (intrusion resistant)

Regelkonform trotz Fehlfunktion
eines Systemteils.

Grundrechtsverträgliche DRM-Systeme gesucht

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

Systeme zur digitalen Rechtekontrolle ... hinken weit hinter den Anforderungen her, beklagten mehrere Referenten der Tagung „Allianz von Recht und Technik“. ... „Nicht jeder Urheber kann sich beliebig beteiligen, die Systeme sind nicht universell, sie sind nicht nutzerfreundlich, und sie erlauben auch keine anonyme Nutzung,“ kritisierte Wolf-Dieter Lukas, Ministerialdirigent im Bundesforschungsministerium.

Heise 5.5.2006

- Symmetrie
- Öffentlichkeit
- Eigentum & Besitz
- Grundrechte (Bildung)

DRM – Diskussion in der Falle

A) Logische Zuordnung von Rechten

(Eigentum/Recht)

B) Faktischer Vollzug von Verfügungen aus 1.

(Besitz/Macht)

- **B muß A faktisch untergeordnet sein**
- **Teilweise widersprüchliche Anforderungen:**
 - A: sei unabhängig von faktischer Gewalt
 - B: sei faktisch unumgehrbar
- **A bricht B im Zweifel**

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Passiv: Analyse**
(Wahrnehmung, rechtlich folgenlos)
- **Aktiv: Vertragsschluß/Verfügung** (Rechtsfolgen)

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Datum**
- **Autor**
- **Inhalt (Prüfsumme)**
- **Programm/Vertrag (nur für Prozesse)**

Selbst verifizierende Identifikatoren (**OID**):

Prüfsumme als Primärschlüssel

systemunabhängiger Identifikator

Unversehrtheit jederzeit zweifelsfrei überprüfbar

- **Verfügung widerspricht eigenem Willen**
- **Methoden:**
 - Entscheider manipulieren
 - Verlust der Kontrolle: „Trust Set“ enthält andere Personen
 - Entmündigung, unbeschränkte Vertretung
 - Bewußtseinsstörung (Drogen verabreichen)
 - Identitätsdiebstahl
 - Administrative Berechtigungen, DRM-Plattform
- **Selbst~Eigentum und ~Besitz.**
Wie beweisen? ...

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

Übertragung von Rechten / Ansprüchen

- **Nebenbedingung:
Grundrechte / Geschäftsfähigkeit bewahren**




Rechtsfähig: bewußt und eigenverantwortlich
Persönlichkeitsrechte unveräußerlich

Ausgangslage
Anforderungen
amtlich
offen
Lösung
Ansatz
passiv
aktiv
logisch
dinglich
Umsetzung
programmatisch
vertraglich
Leistung

Askemos - Regel

Ausgangslage
 Anforderungen
 amtlich
 offen
Lösung
 Ansatz
 passiv
 aktiv
 logisch
 dinglich
 Umsetzung
 programmatisch
 vertraglich
 Leistung

Universalmenge (alle Objekte)	$a \in A$
Menge der Nutzer	$n \in N \subset A$
Menge der Informationen die n hat	$S_n \subset A$
Menge R aller Rechte r zu n	$r \in R \wedge R \subset S_n$
Selbsteigentum	$n \in R$
Weitergabe (grant):	$r_g \subset r$  r'
	$\forall t \in r_g (t \mid t \in r \wedge t \in r')$

Fazit: nicht korrumpierbar heißt:

$$\neg(r \setminus r_g) = \emptyset$$

= Gilt für jedes System von Rechten. =

Ausgangslage
Anforderungen

amtlich
offen

Lösung

Ansatz
passiv
aktiv

logisch

dinglich

Umsetzung

programmatisch
vertraglich

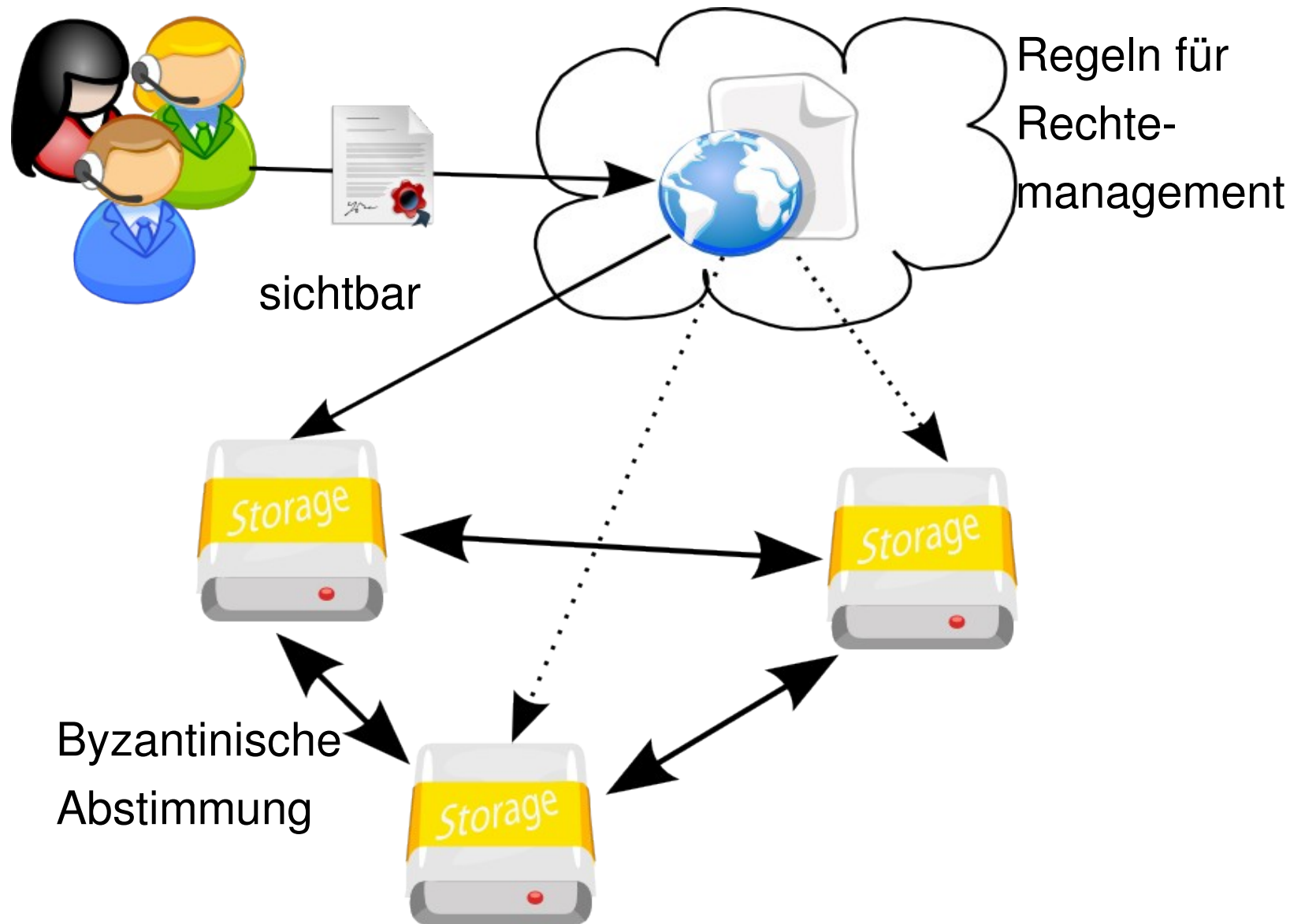
Leistung



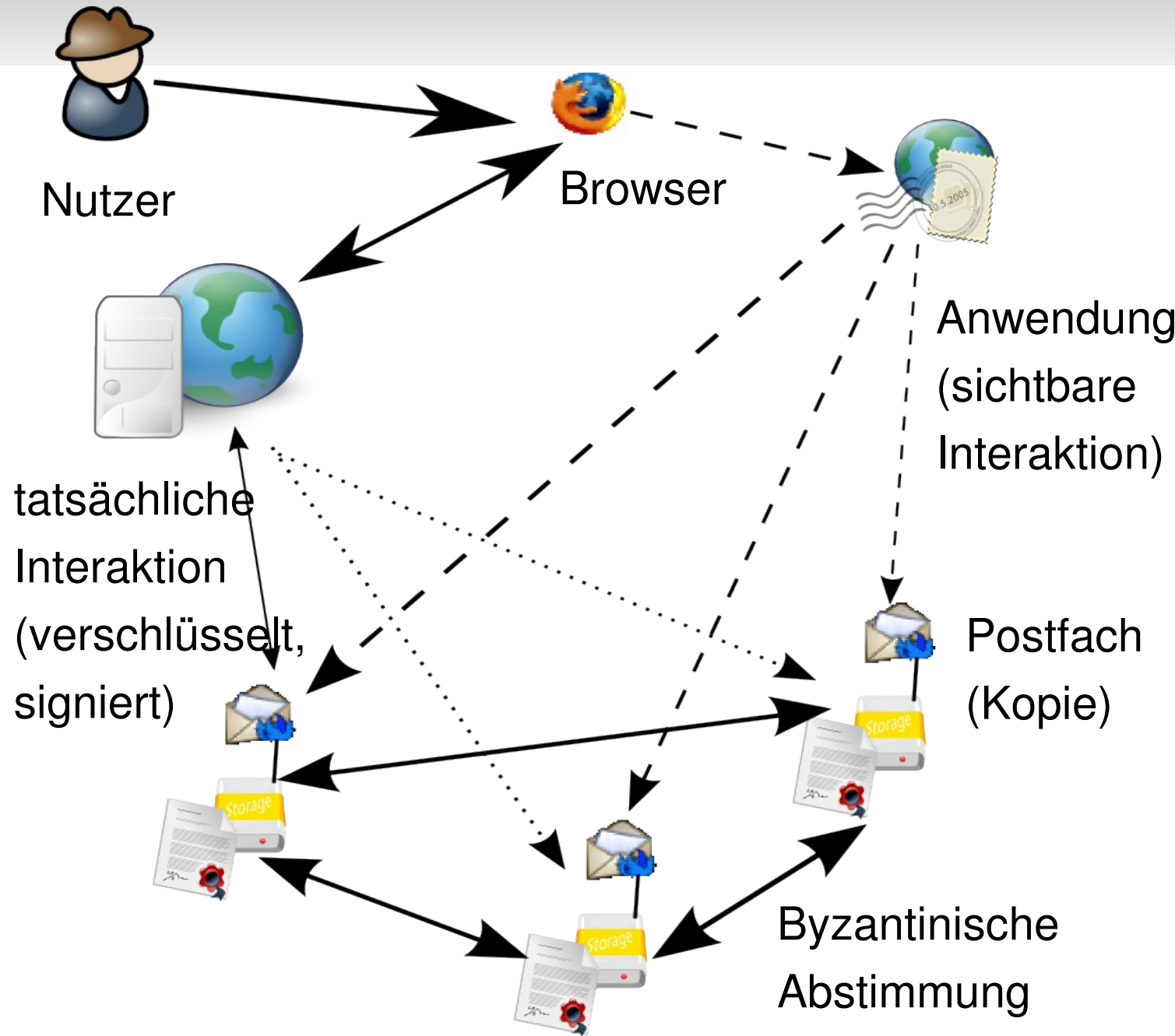
- **100% Sicherheit garantiert unmöglich**
- **garantiert 0 Sicherheit mit Single Point of Failure**
 - Maschinen
 - Andere Personen
 - Eigenes Versagen (Epressung, Verwirrung)

Byzantine Einigung

Ausgangslage
Anforderungen
amtlich
offen
Lösung
Ansatz
passiv
aktiv
logisch
dinglich
Umsetzung
programmatisch
vertraglich
Leistung



eEinschreiben



Ausgangslage
Anforderungen

amtlich
offen

Lösung

Ansatz
passiv
aktiv

logisch

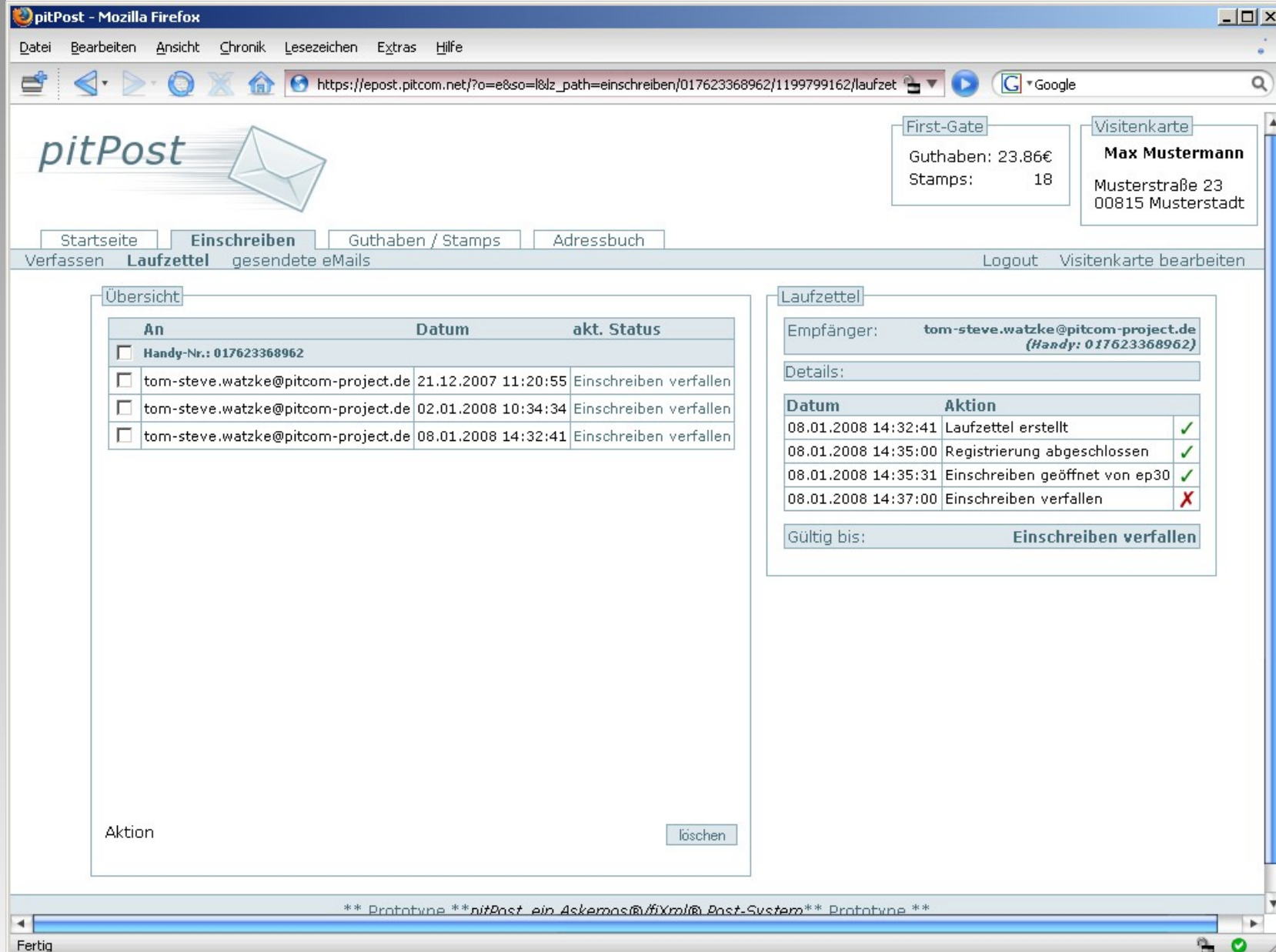
dinglich

Umsetzung
programmatisch
vertraglich

Leistung

eEinschreiben mit Rückschein

Ausgangslage
 Anforderungen
 amtlich
 offen
Lösung
 Ansatz
 passiv
 aktiv
 logisch
dinglich
 Umsetzung
 programmatisch
 vertraglich
 Leistung



First-Gate
 Guthaben: 23.86€
 Stamps: 18

Visitenkarte
Max Mustermann
 Musterstraße 23
 00815 Musterstadt

Startseite | **Einschreiben** | Guthaben / Stamps | Adressbuch
 Verfassen | **Laufzettel** | gesendete eMails | Logout | Visitenkarte bearbeiten

Übersicht

An	Datum	akt. Status
<input type="checkbox"/> Handy-Nr.: 017623368962		
<input type="checkbox"/> tom-steve.watzke@pitcom-project.de	21.12.2007 11:20:55	Einschreiben verfallen
<input type="checkbox"/> tom-steve.watzke@pitcom-project.de	02.01.2008 10:34:34	Einschreiben verfallen
<input type="checkbox"/> tom-steve.watzke@pitcom-project.de	08.01.2008 14:32:41	Einschreiben verfallen

Aktion löschen

Laufzettel
 Empfänger: tom-steve.watzke@pitcom-project.de
 (Handy: 017623368962)

Details:

Datum	Aktion	
08.01.2008 14:32:41	Laufzettel erstellt	✓
08.01.2008 14:35:00	Registrierung abgeschlossen	✓
08.01.2008 14:35:31	Einschreiben geöffnet von ep30	✓
08.01.2008 14:37:00	Einschreiben verfallen	✗

Gültig bis: **Einschreiben verfallen**

** Prototypne ** nitPost ein Askemas@fiXml@ Post-System ** Prototypne **

Fertig

Prozesse und Vertragsfreiheit

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmlich

vertraglich

Leistung

- **Gesetze und Verträge = Rahmenbedingungen für Prozesse**
- **Mathematisch:**
Kalküle für parallele Vorgänge
Wahl: Pi-Kalkül
- **Pi-Kalkül funktioniert in Schritten**
 - Gelegenheit zur byzantinischen Einigung
- **Vertragsfreiheit bedeutet:**
freie Benutzung mathematischer Kalküle!

Rechenleistung aus der Steckdose

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

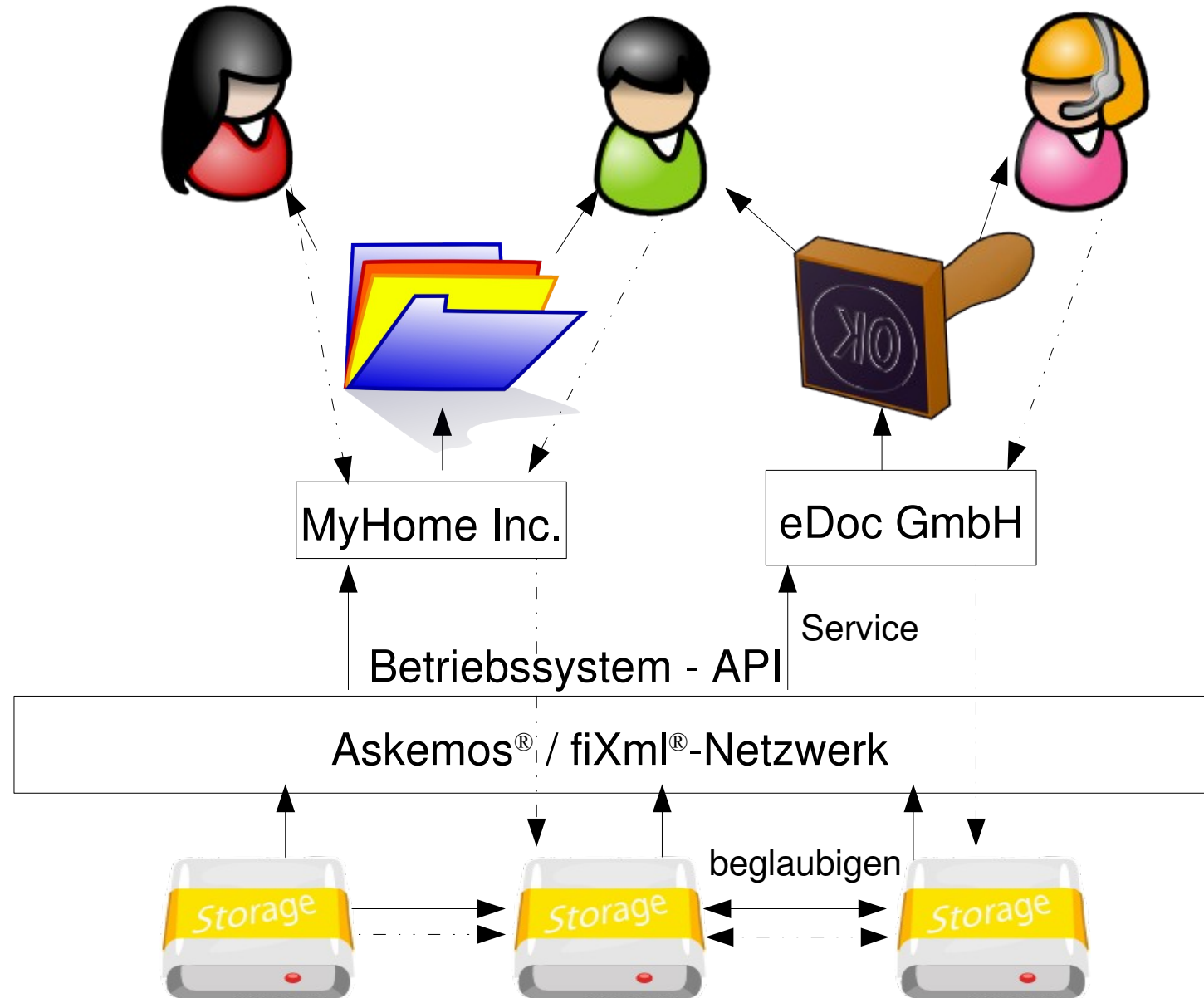
dinglich

Umsetzung

programmatisch

vertraglich

Leistung



Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Nicht rechtsverbindlich. Sorry.**
- **Provider geschickt wählen!**
 - Gesundheit: Arzt, Apotheker, ich
 - Einkommen: Bank, Arbeitgeber, ich
 - Tagebuch: sag' ich nicht
- **Hohe Wertkonzentration vermeiden!**

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- Derzeit unklare Rechtslage
- Provider gleich Benutzer
- Netzverbindung ungleich Kommunikationsvorgang
- Viele Verbindungen
fast nur Prüfsummen
-> kaum aussagekräftig
- Nur Garbage-Collector abschalten?
- Askemos ist *kein* Anonymisierungsdienst

- herkömmlicher Vertragsschluss für elektronische Kommunikation
- Beweiswertes gegenüber der qualifizierten elektronischen Signatur verbessert
- **Mehrfache Identifizierung** erhöht Sicherheit, Annahme zumindest eines Anscheinsbeweises gerechtfertigt.
- Ausreichende **Sicherheit an Authentizität** und Integrität für Anscheinsbeweis.
- keine gesetzlichen Beweiserleichterungen (Gründe für diese Entscheidung des Gesetzgebers sind nicht ersichtlich.)
- **Gutachten RA Markus Heinker, Kanzlei Dr. Fingerle**

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- wie Internet – im Browser
oder: ein neues Daten-Laufwerk
- geschlossenes „social network“
- aktuelle Software
- Ein (verschlüsseltes) Verzeichnis
z.B. USB-Stick oder Askemos-
Netzlaufwerk

- Zuverlässiger, verantwortlicher **Dienst**.
- Unabhängigkeit von Ort und Anbieter, Einsatzbereich ist Vertragssache
- Dienstleistung bei Personalisierung und Aktualisierung
(wiederkehrender Kundenkontakt mit Nutzern).
- Neuartige Leistungsmerkmale:
revisionssichere Prozesse
- Copyright-Verletzungen verfolgbar.
- Aktuelle, gepflegte Software.
- Kostengünstig, kein Medienbruch.

- Applikation-Server – bekannte Technik
- Clientsoftware leicht aktualisierbar
- Qualitätssprung, neue Leistungen
- Stetiges, pauschales Geschäft
- Qualitativ hochwertiges Massenprodukt

Für Provider

- Öffentlich verifizierbar ohne Hintertür
- Dual-Lizenz (GPL und proprietär)
- Gesetzesänderungen?
 - kein Bedarf
(Überregulierung überflüssig)
 - keine Gefahr

Ausgangslage

Anforderungen

amtlich

offen

Lösung

Ansatz

passiv

aktiv

logisch

dinglich

Umsetzung

programmatisch

vertraglich

Leistung

- **Pi-Kalkül**
 - Mutation: implizit
 - Nachrichten: <send>, <fetch>
- **Topologie- / Namensmanagement**
 - <link>
 - <new>
- **Rechtmanagement**
 - <grant>, <revoke>
- **Integration technischer Dienste**
 - <TrustedCode>, <secret>

Ausgangslage
Anforderungen
amtlich
offen
Lösung
Ansatz
passiv
aktiv
logisch
dinglich
Umsetzung
programmatisch
vertraglich
Leistung

- **HTTP/S, WebDAV, Mail**
- **Web 1.5; Web 2.0 tauglich**
- **Einschreiben, SMS, Wiki, Foren**
- **WAN-Update < 0,4 s (Verhältnis zu BSI-Bedarf wie 170000:6000)**
- **optimiert für XML, Unicode und „plain file“**
- **>94% transaktionsverfügbar in <5 s**
 - Entwicklungsnetzwerk simuliert 25% Ausfall
- **99,999% leseverfügbar**

- Ausgangslage
- Anforderungen
 - amtlich
 - offen
- Lösung
- Ansatz
 - passiv
 - aktiv
 - logisch
 - dinglich
- Umsetzung
 - programmatisch
 - vertraglich
- Leistung



Dienstleistungsarchitektur für Compliance-Prozesse

Startseite Projekt Verbund Veröffentlichungen

Login Impressum Kontakt

Navigation

- Projekt
- Verbund
- Veröffentlichungen

BMBF-Verbundvorhaben

Compliance-Anforderungen wie ISO 17799, ISO 27001, IT-Grundschutz oder SOX sind längst nicht nur ein Thema weltweit agierender Großkonzerne. Compliance über die Gesamtheit der Geschäftsprozesse. Risiken feststellen - gesetzliche und normative Auflagen erfüllen.
- ein Thema auch für KMU -



Dieses Forschungs- und Entwicklungsprojekt wird mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) innerhalb des Rahmenkonzeptes 'Forschung für die Produktion von morgen' gefördert.



Kalender						
<	Januar 2008					>
Mo	Di	Mi	Do	Fr	Sa	So
0	31	1	2	3	4	5
1	7	8	9	10	11	12
2	14	15	16	17	18	19
3	21	22	23	24	25	26
4	28	29	30	31	1	2

Ausgangslage
 Anforderungen
 amtlich
 offen
 Lösung
 Ansatz
 passiv
 aktiv
 logisch
 dinglich
 Umsetzung
 programmatisch
 vertraglich

Leistung

<https://login.softeyes.net/A8ff33a61be3927d6d3495fa7b9b515a5?fid=1>

DLA-Forum

 Hallo rahe

 Optimiert für: Firefox

Foren		<input type="button" value="neues Forum"/>	Themen	Beiträge	Letzter Beitrag
-	Allgemeines Hier kommen allgemeine Informationen hinein.	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	5	6	09.01.2008 10:02:01 von rahe
		<input type="button" value="neues Thema"/>	<i>Letzter Beitrag</i>		
	Arbeitspaket 1	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	2	09.01.2008 09:00:21 von rahe	
	Arbeitspaket 2	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	1	09.01.2008 09:01:22 von rahe	
	Arbeitspaket 3	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	1	09.01.2008 09:01:37 von rahe	
	Arbeitspaket 4	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	1	09.01.2008 09:01:51 von rahe	
	Arbeitspaket 5	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	1	09.01.2008 09:02:01 von rahe	
+	Askemos Referenz Hier darf alles rein, was zur Dokumentation Askemos' dient.	<input type="button" value="löschen"/> <input type="button" value="bearbeiten"/>	0	0	

<http://www.dla-compro.de/A8ff33a61be>

Fehlermanagement KFZ-Fertigung

Ausgangslage
Anforderungen
amtlich
offen
Lösung
Ansatz
passiv
aktiv
logisch
dinglich
Umsetzung
programmatisch
vertraglich
Leistung



CFMSys

Collaboratives Fehler-Management-System

Startseite Projekt Verbund Veröffentlichungen

Login Impressum Kontakt

Navigation

- Projekt
- Verbund
- Veröffentlichungen

BMW-Vorhaben

unternehmensübergreifende Steuerung der Fehlerbehebungsprozesse in der
Automobilzulieferindustrie NBL
- webbasiert - rückverfolgbar - reversionssicher -



Bundesministerium
für Wirtschaft
und Technologie

Dieses Forschungs- und Entwicklungsprojekt wird mit Mitteln des Bundesministeriums für Wirtschaft und Technologie (BMWi) innerhalb des Rahmenkonzeptes 'Förderung von Forschung und Entwicklung bei Wachstumsträgern in benachteiligten Regionen' gefördert.



Kalender

< Januar 2008 >

	Mo	Di	Mi	Do	Fr	Sa	So
0	31	1	2	3	4	5	6
1	7	8	9	10	11	12	13
2	14	15	16	17	18	19	20
3	21	22	23	24	25	26	27
4	28	29	30	31	1	2	3

WebDAV-Verzeichnis

Ausgangslage
Anforderungen
amtlich
offen
Lösung
Ansatz
passiv
aktiv
logisch
dinglich
Umsetzung
programmatisch
vertraglich
Leistung

```
jfw@gus: /home/jfw
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
jfw@gus:~$ ls -l Askemos/AskemosWebsite.dir
insgesamt 8505
-rw-r--r-- 1 jfw jfw 252416 2005-02-23 22:11 200502-PitVorAskemosCode.jpg
-rw-r--r-- 1 jfw jfw 26890 2005-06-08 20:35 20050504-Chemnitz.sxw
-rw-r--r-- 1 jfw jfw 1196951 2007-02-15 01:16 askemos-0.8.2.tar.gz
-rw-r--r-- 1 jfw jfw 1221033 2007-04-18 23:20 askemos-0.8.3.tar.gz
-rw-r--r-- 1 jfw jfw 1239500 2007-05-30 18:59 askemos-0.8.4.tar.gz
-rw-r--r-- 1 jfw jfw 588 2007-09-12 13:28 Askemos Forum
-rw-r--r-- 1 jfw jfw 1166590 2007-09-26 13:18 askemos-new.tar.gz
-rw-r--r-- 1 jfw jfw 1124270 2008-01-09 18:03 askemos.tar.gz
drwxr-xr-x 3 jfw jfw 4096 2008-01-08 19:08 Askemos.wiki
drwxr-xr-x 3 jfw jfw 4096 2008-01-07 18:41 Background Library.dir
-rw-r--r-- 1 jfw jfw 159281 2006-04-23 14:24 chicken-ball.tar.gz
-rw-r--r-- 1 jfw jfw 863026 2006-09-08 16:53 Christian Thiele - Diplomarbeit.pdf
f
drwxr-xr-x 3 jfw jfw 4096 2008-01-07 18:50 documentation
drwxr-xr-x 3 jfw jfw 4096 2008-01-07 18:54 examples
-rw-r--r-- 1 jfw jfw 5448 2004-09-23 16:39 full.dia
-rw-r--r-- 1 jfw jfw 34282 2004-09-23 16:40 full.png
-rw-r--r-- 1 jfw jfw 5588 2008-01-09 15:04 GlobalClock
-rw-r--r-- 1 jfw jfw 7286 2007-10-06 20:55 GlobalReminder
-rw-r--r-- 1 jfw jfw 486 2008-01-09 15:04 GlobalReminderRun
drwxr-xr-x 3 jfw jfw 4096 2008-01-08 19:08 index.html
-rw-r--r-- 1 jfw jfw 3140 2004-09-23 16:40 integration.html
-rw-r--r-- 1 jfw jfw 395 2007-11-27 16:43 linie.png
-rw-r--r-- 1 jfw jfw 6736 2004-09-23 16:40 modelling.html
-rw-r--r-- 1 jfw jfw 3307 2004-09-23 16:41 network.dia
-rw-r--r-- 1 jfw jfw 27287 2004-09-23 16:41 network.png
-rw-r--r-- 1 jfw jfw 1270062 2007-07-08 15:30 N.Luhmann-Vertrauen.pdf
-rw-r--r-- 1 jfw jfw 1973 2004-09-23 16:43 overview.html
-rw-r--r-- 1 jfw jfw 3280 2004-09-23 16:41 petri-model.dia
-rw-r--r-- 1 jfw jfw 23585 2004-09-23 16:41 petri-model.png
drwxr-xr-x 3 jfw jfw 4096 2008-01-07 18:56 skin
drwxr-xr-x 3 jfw jfw 4096 2007-08-20 19:17 stylelib
-rw-r--r-- 1 jfw jfw 103 2007-11-27 16:38 tlxl.png
-rw-r--r-- 1 jfw jfw 2376 2004-09-23 16:42 user.dia
-rw-r--r-- 1 jfw jfw 24175 2004-09-23 16:43 user.png
-rw-r--r-- 1 jfw jfw 3538 2004-09-23 16:42 user-view.html
jfw@gus:~$
```

**Der globale Computer ist kein
Objekt, er ist eine Eigenschaft.**

[Ben Howel Davis]