Rechtsicherheit im elektronischen Geschäftsverkehr

Jörg Wittenberger
Softeyes GmbH
Erlenstraße 22
01097 Dresden

joerg.wittenberger@softeyes.net

Der „IST“ - Zustand

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

joerg.wittenberger@softeyes.net

Rechtliche Anforderungen

- **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**

joerg.wittenberger@softeyes.net

Grundsätzliche Anforderungen

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

Bundesamt für Sicherheit in Informationstechnik

joerg.wittenberger@softeyes.net

softeyes

Trusted...

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.

joerg.wittenberger@softeyes.net

elektronische Unterschrift

Exkurs

joerg.wittenberger@softeyes.net

elektronische Unterschrift

Exkurs

joerg.wittenberger@softeyes.net

softeyes

Zentral Verrechnet

Zertifizierer

§11 SigG: schuldhafte Pflicht- & Produkthaftung
§12 ≤250.000 € je Fall *geeignete Deckungsvorsorge*

Notare

§ 19 BNotO: persönlich, unbeschränkbar Haftung
§ 19a(3): ≥500.000 € je Fall, ≥2xpro Jahr versichert

- Wie versichern?
  Vorsatz – Pishing – Fortschritt
- Wenige Zertifizierer – viele Kunden
  - hoher Wert im Schlüssel
  - oft gebraucht
  - leicht korrumpierbar

joerg.wittenberger@softeyes.net

softeyes

Logische Zuordnung sei

nicht korrumpierbar (nicht manipulierbar)

Kein Individuum kann ein anderes verkörpern.

störfest (intrusion resistant)

Regelkonform trotz Fehlfunktion eines Systemteils.

joerg.wittenberger@softeyes.net

Grundrechtsverträgliche DRM-Systeme gesucht

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)

joerg.wittenberger@softeyes.net

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 unumgehbar
- **A bricht B im Zweifel**

joerg.wittenberger@softeyes.net

softeyes

Zwei Modi

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

joerg.wittenberger@softeyes.net

Urkunden

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

Selbst verifizierende Identifikatoren (OID):
Prüfsumme als Primärschlüssel
systemunabhängiger Identifikator
Unversehrtheit jederzeit zweifelsfrei überprüfbar

joerg.wittenberger@softeyes.net

softeyes

Korruption

- **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? ...

joerg.wittenberger@softeyes.net

Übertragung von Rechten / Ansprüchen

- **Nebenbedingung:**
  Grundrechte / Geschäftsfähigkeit bewahren

Rechtsfähig: bewußt und eigenverantwortlich
Persönlichkeitsrechte unveräußerlich

joerg.wittenberger@softeyes.net

Askemos - Regel

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): $r_g \subset r$ kopieren 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. =

joerg.wittenberger@softeyes.net

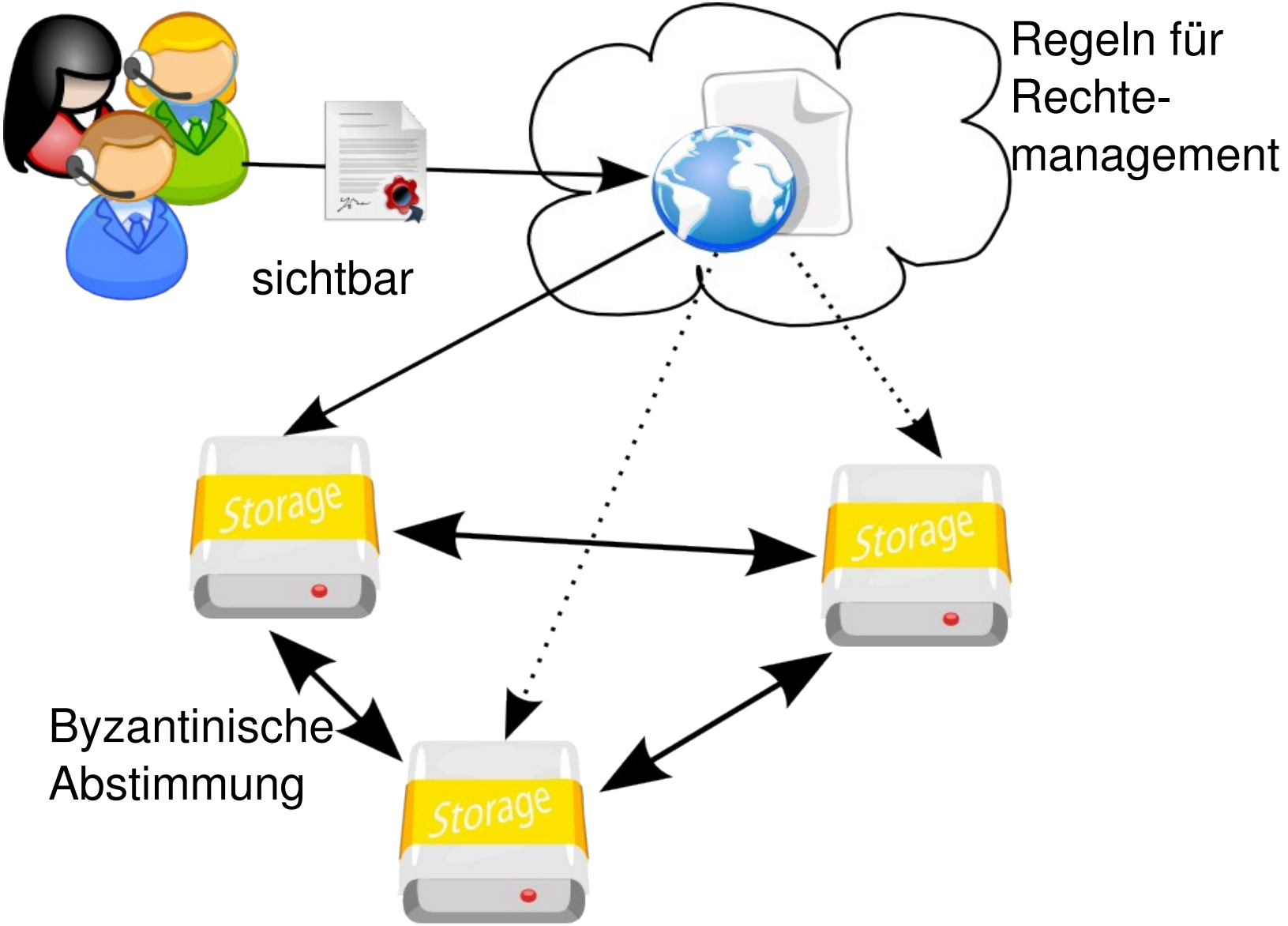
Störung

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

joerg.wittenberger@softeyes.net

Byzantine Einigung

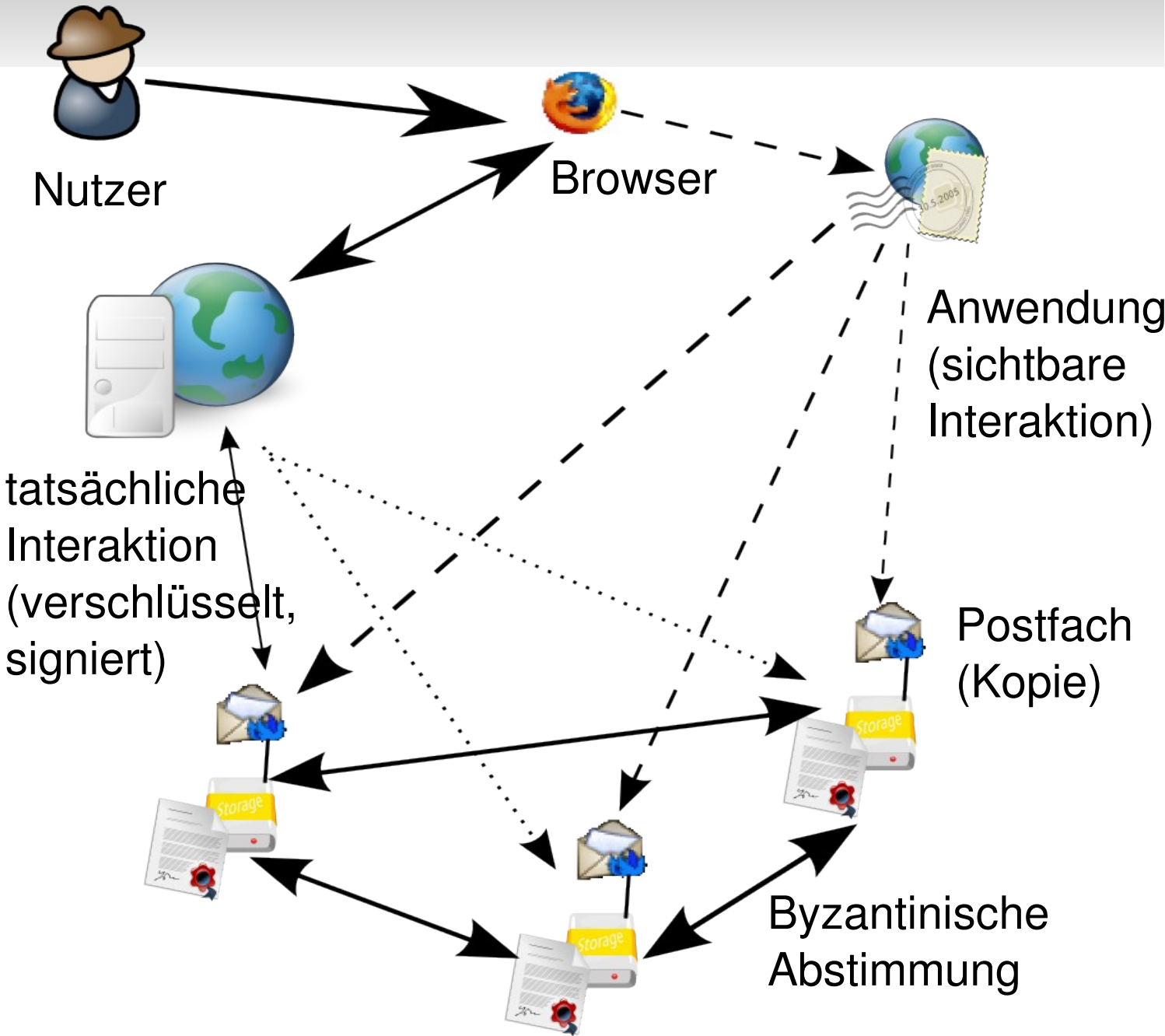
- Ausgangslage
- Anforderungen
  - amtlich
  - offen
- **Lösung**
  - Ansatz
  - passiv
  - aktiv
    - logisch
    - **dinglich**
- Umsetzung
  - programmatisch
  - vertraglich
- Leistung



joerg.wittenberger@softeyes.net

eEinschreiben

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



joerg.wittenberger@softeyes.net

softeyes

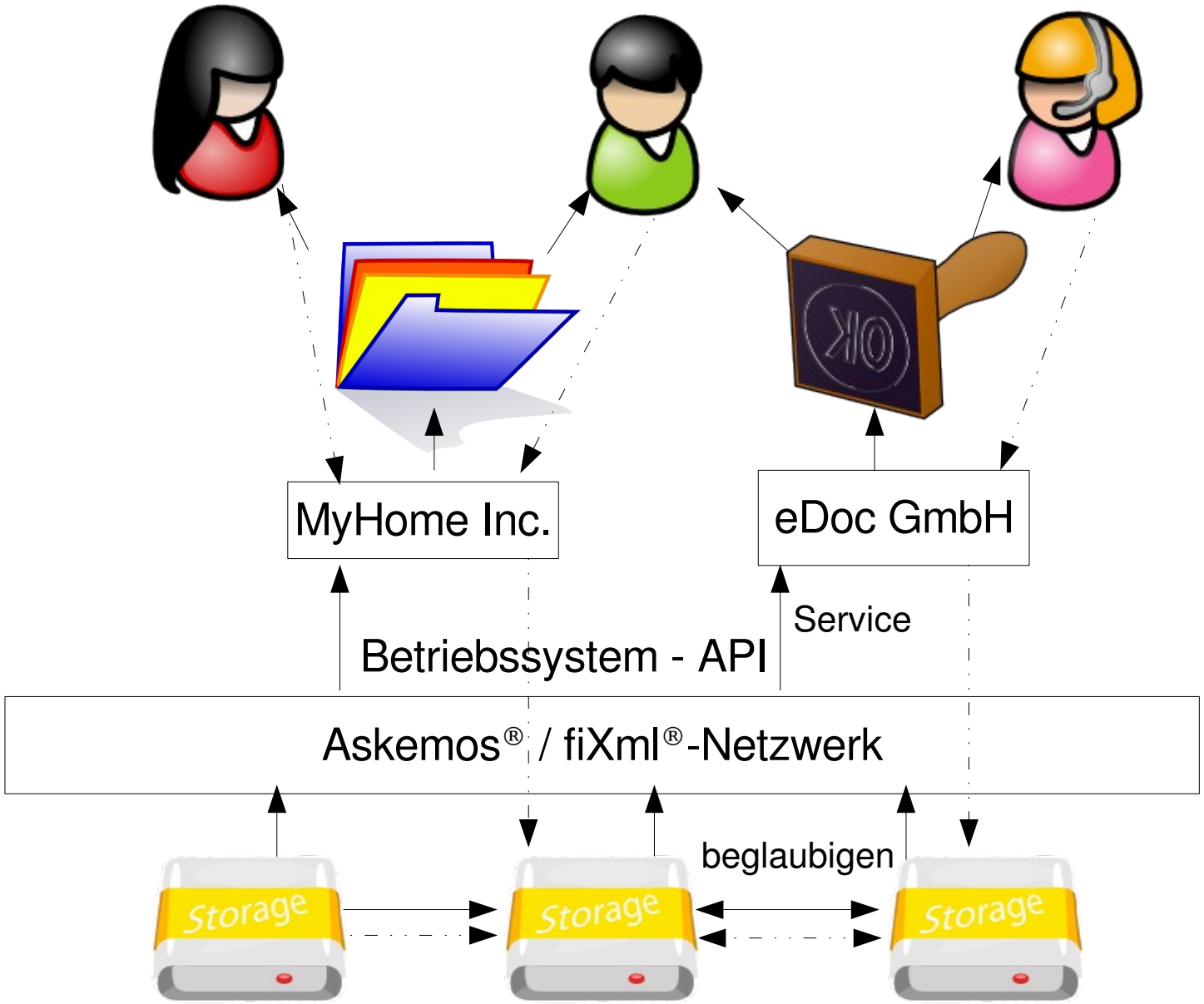
Prozesse und Vertragsfreiheit

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

joerg.wittenberger@softeyes.net

Rechenleistung aus der Steckdose

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



joerg.wittenberger@softeyes.net

Geheimnisse?

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

joerg.wittenberger@softeyes.net

softeyes

einfaches API

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

joerg.wittenberger@softeyes.net

softeyes

Praxis

- 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“
- >96% transaktionsverfügbar in <5 s
  - Entwicklungsnetzwerk simuliert 25% Ausfall
- 99,999% leseverfügbar

joerg.wittenberger@softeyes.net

softeyes

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

[Ben Howel Davis]

Jörg Wittenberger
Softeyes GmbH
Erlenstraße 22
01097 Dresden

joerg.wittenberger@softeyes.net