TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik | Institut Systemarchitektur | Professur Rechnernetze

WS 2011
LV Informatik-I für Verkehrsingenieure

8. Verteilte Systeme Applikationsprobleme

Dr. rer.nat. D. Gütter

Mail: Dietbert.Guetter@tu-dresden.de
WWW: wwwpub.zih.tu-dresden.de/~guetter/

Verteilte Verarbeitung

Arbeit von Systemen, bei denen ein Anwendungsdienst durch Zusammenwirken mehrerer Prozesse erbracht wird.

Havarieverbund
Realisierung der Nutzeraufträge auch bei Computerausfällen

Lastverbund
höherer Auftragsdurchsatz

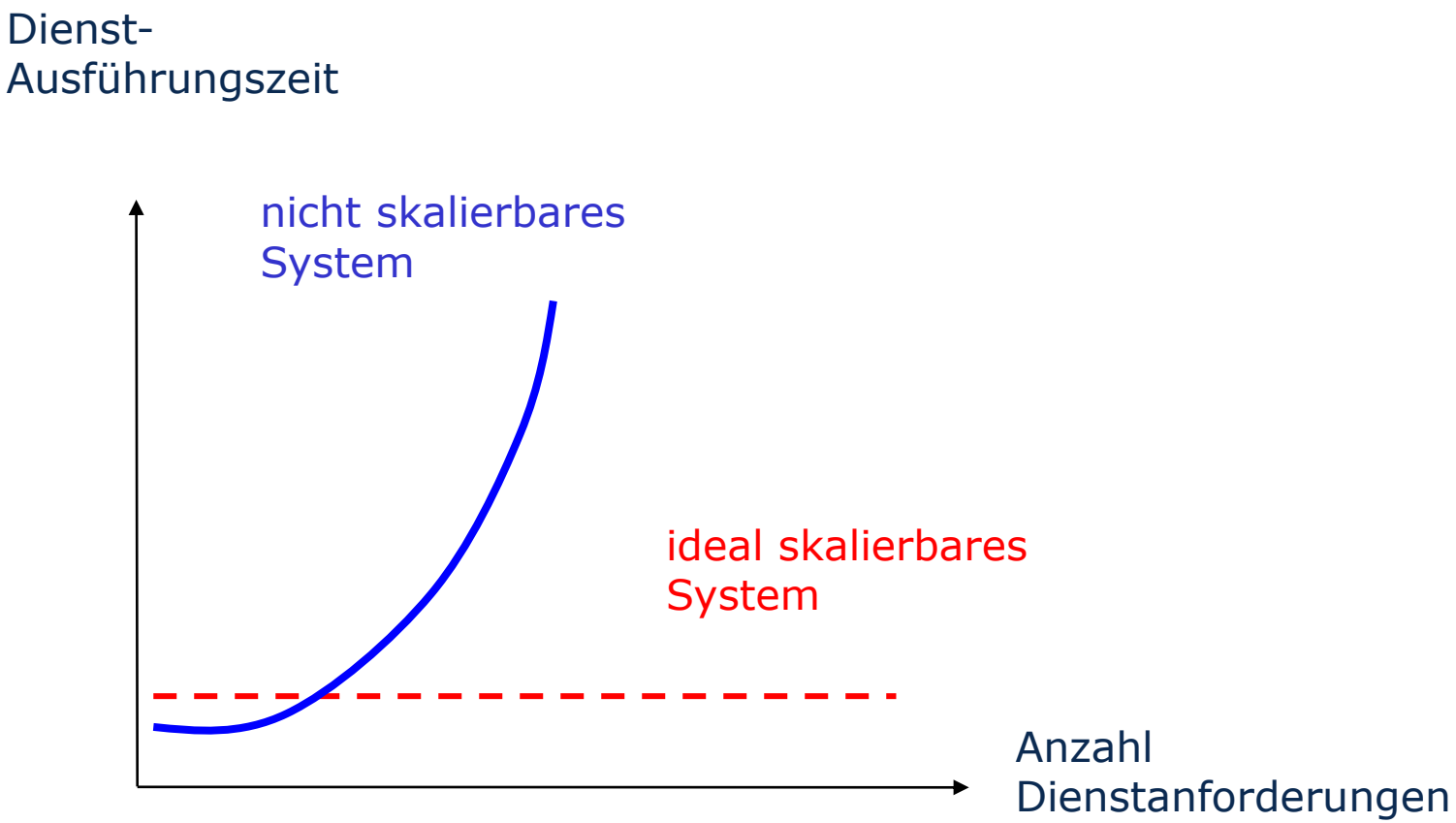
Funktionsverbund
Nutzung von Dienstleistungen anderer Computer

Datenverbund
Entfall kosten- und zeitaufwendiger Datentransporte

Ressourcenverbund
Einsparung von Investitionen

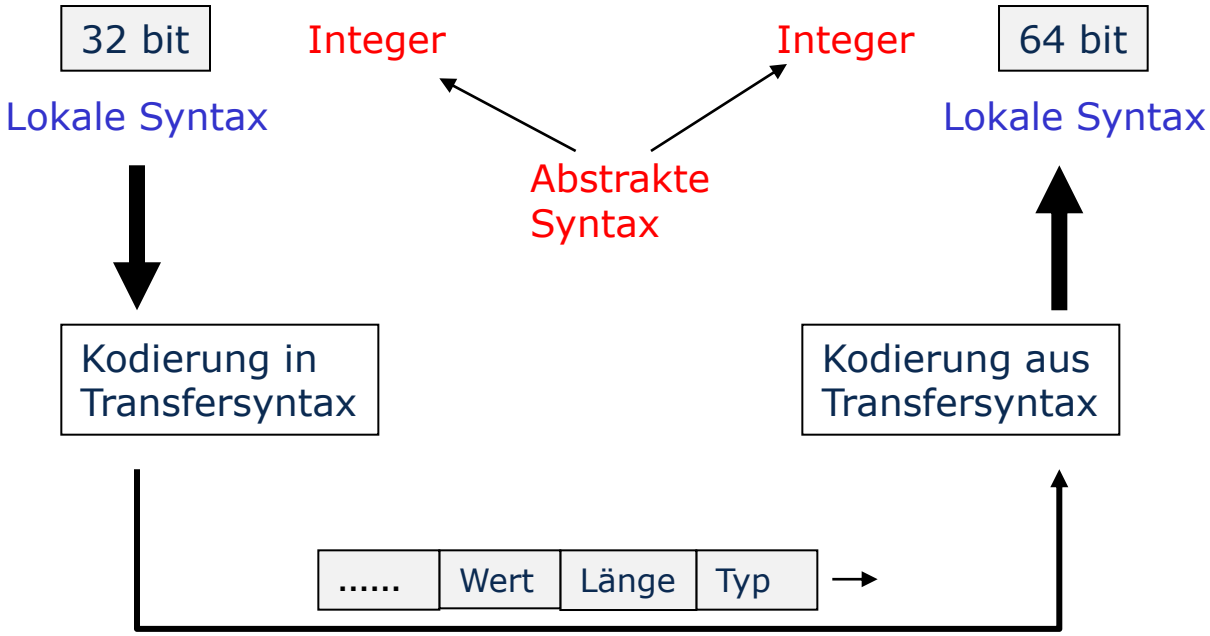
→ Client –Prozesse für Dienstanforderung
Server-Prozesse für Diensterbringung

Skalierbarkeit



Informationsdarstellung

Informationsaustausch in **heterogenen** Systemen



Übertragung in **Transfersyntax**

z.B. in **XML** (Extensible Markup Language)

Datenkompression

Entropiekodierung

Kompaktere, redundanzfreiere Darstellung
kontext- und verlustfrei, medienunabhängig

- von Zeichenwiederholungen durch Angabe
- von Zeichen unterschiedlicher Auftrittswahrscheinlichkeit durch unterschiedlich lange Bitfolgen (Huffman-Algorithmus)
- mehrfach auftretenden Zeichenfolgen durch Substitution

Quellenkodierung

kontext- und verlustbehaftet, medienabhängig

- Nutzung z.B. für Sprach- und Videoübertragungen

Hybrid

z.B.

- JPEG (Joint Pictures Expert Group) für Einzelbilder
- MPEG (Motion Picture Expert Group) für Video

Sicherheitsaspekte

besondere Bedeutung
bei Übermittlung von Verträgen, Dokumenten oder Zahlungsanweisungen

Anforderungen

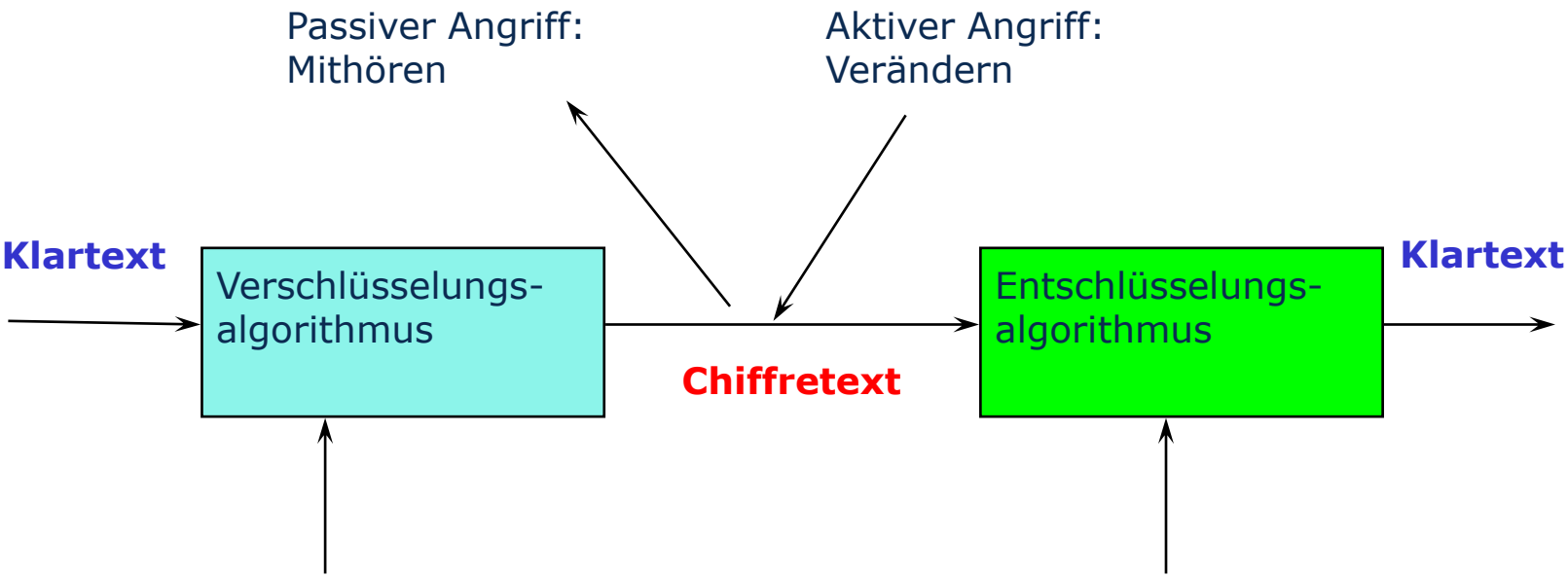
- Integrität der Meldungen
- Überprüfbarkeit des Absenders (Authentisierung)
- Vertraulichkeit der übermittelten Meldungen
- Schutz vor Verlust oder Verdopplung von Meldungen

Eingriffsmöglichkeiten

- Mitlesen/Modifizieren von Datenpaketen
- Leitungsunterbrechungen
- Maskerade (Vortäuschen falscher Identität)
- Falsche Weiterleitung, Stören von Systemen etc.

Kryptographie (Verschlüsselung)

Verschlüsselungsmethode meist nicht geheim !



Symmetrische Verfahren: K=K';
Asymmetrische Verfahren: K#K'

Kryptoverfahren

Allgemein

- Sicherheit der Krypto-Algorithmen muss gewährleistet sein.
- Schlüsselverteilung muss sicher sein.
- Ein Testen aller möglichen Schlüssel (brute force) muss so aufwendig sein, dass es praktisch nicht möglich ist.
  (→ ausreichende Schlüssellänge)

Symmetrische Verfahren

- schnelle Algorithmen

- nachteilig

  Sender und Empfänger müssen gleichen Schlüssel kennen.
  Dem Empfänger muß vertraut werden (Schlüsselweitergabe).
  Schlüssel können nur über sichere Zweitkanäle verteilt werden.

- Beispiele: DES, IDEA, AES

Kryptoverfahren (2)

Asymmetrische Verfahren

- Schlüssel K für Verschlüsselung kann veröffentlicht werden!
  (einfache Schlüsselverteilung)
- neuartige Möglichkeiten (Elektronische Unterschriften, Zertifikate, …)

- nachteilig: Algorithmen sind langsam

- Beispiele: RSA (Rivest, Shamir, Adleman), Diffie-Hellman

Kombination beider Verfahren

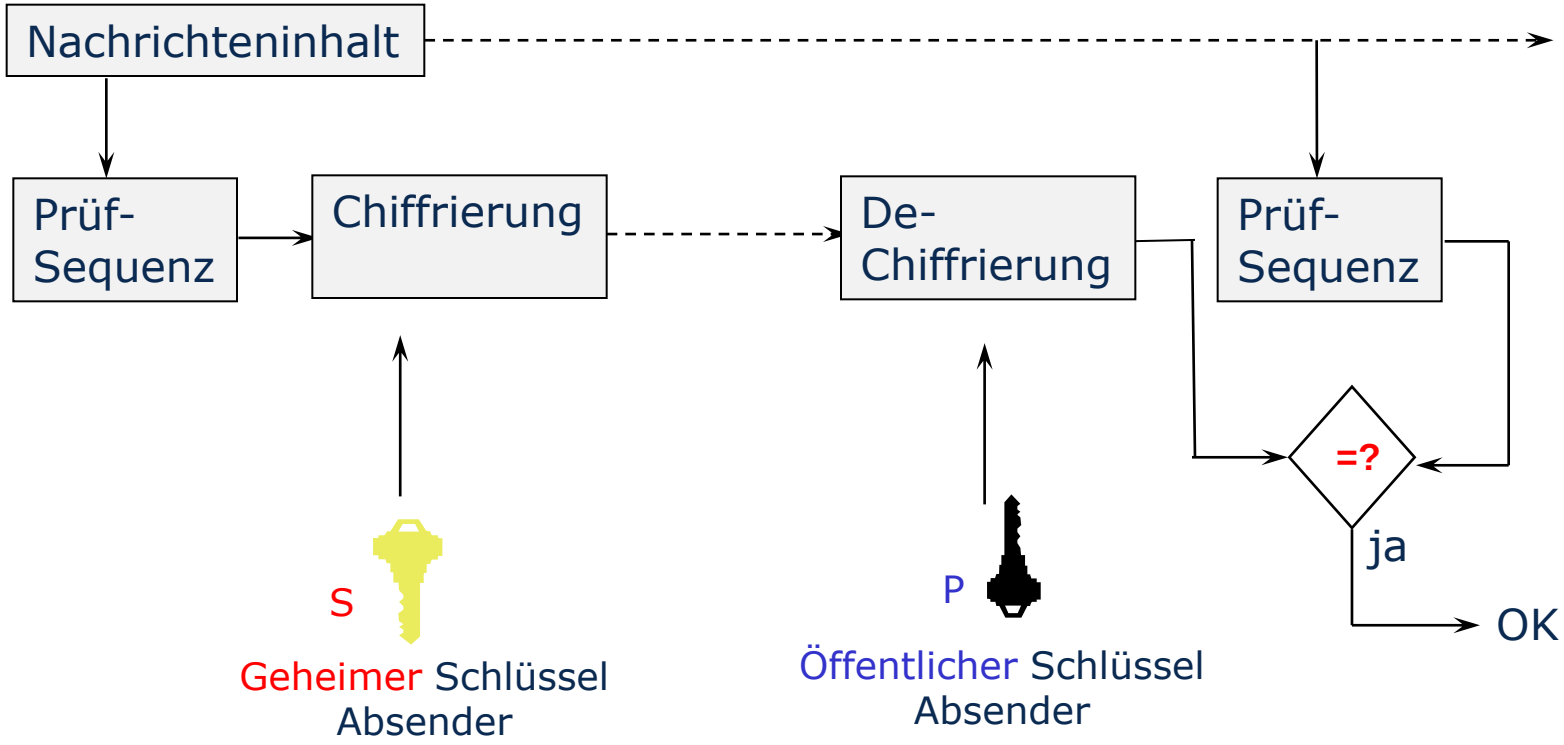
- Schlüsselgenerierung
  zweier asymmetrischer Schlüssel (privater und öffentlicher Schlüssel)
  und eines temporären symmetrischen Schlüssels

- Schlüsselübertragung durch asymmetrisches Verfahren
  Übertragung der Inhalte durch ein symmetrisches Verfahren

Digitale Unterschrift (gesetzlich anerkannt)

Prinzip

Prüfsumme über gesamten Inhalt bilden
Asymmetrische Verschlüsselung mit privatem Schlüssel des Senders
Empfänger prüft Authentizität des Senders und Integrität der Nachricht



Integrität öffentlicher Schlüssel

Problem
Nachweis der Zuordnung von Benutzername und Schlüssel
(Maskerade)

Vergleich
Nachweis der Zugehörigkeit eines Ausweises zu einer Person (Lichtbild)

Lösungsmöglichkeiten

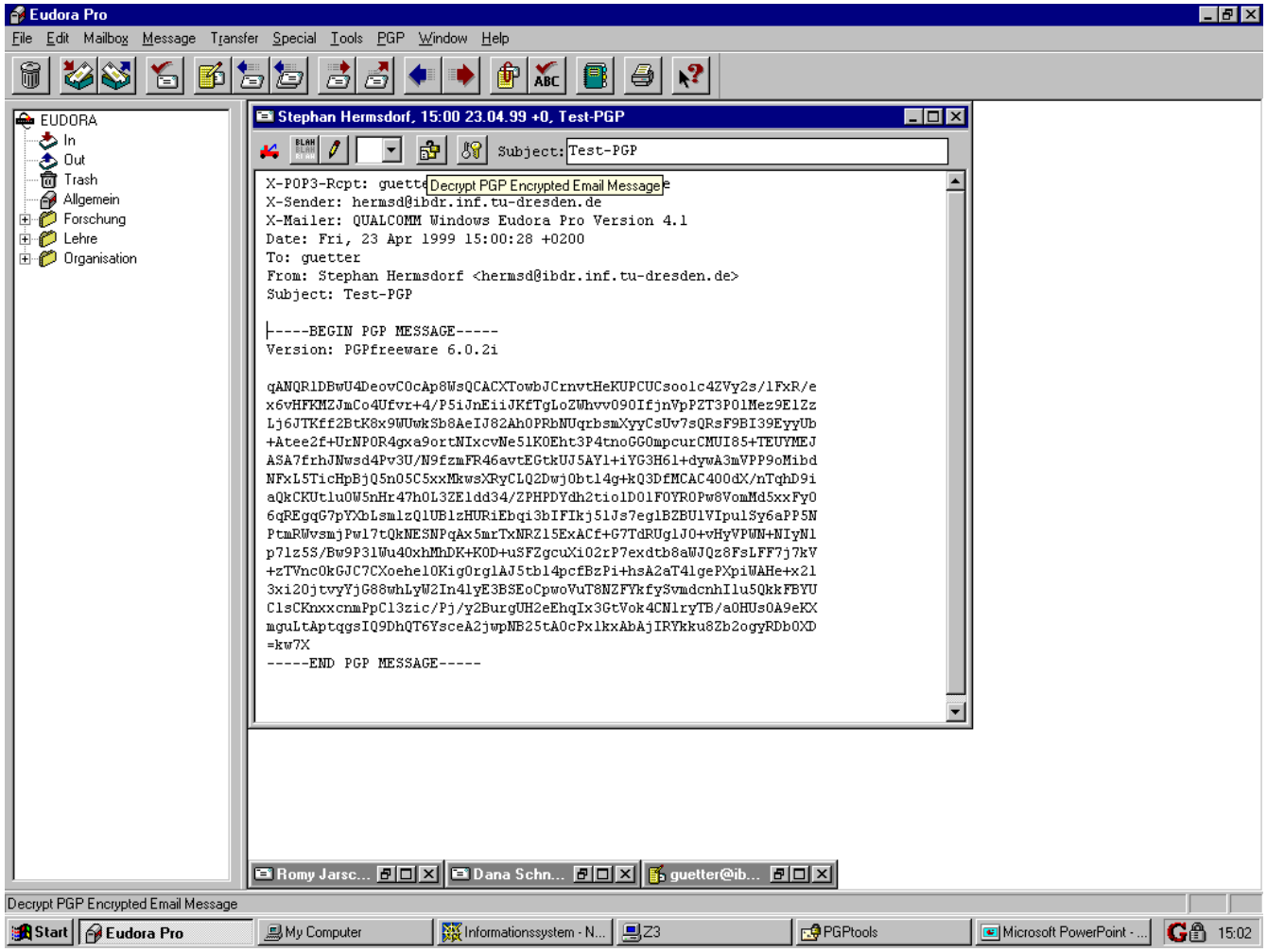
- Verteilung von Namen/Schlüsseln über alternative sichere Kanäle.
- Verteilung über normale Netze mit **Zertifikat**

  Inhalt: Name, öffentlicher Schlüssel
  Algorithmus zur Chiffrierung
  Gültigkeitsdauer

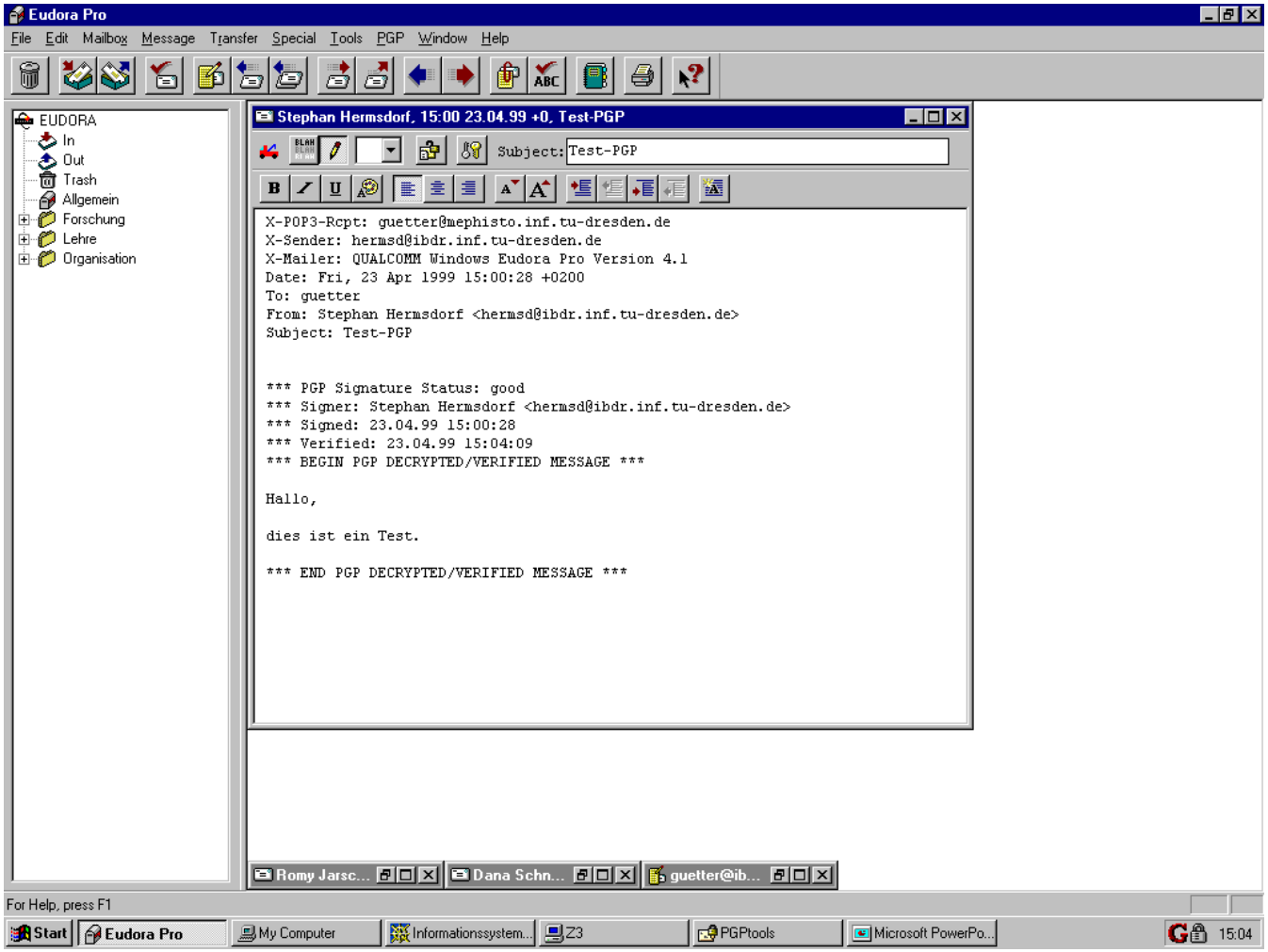
  + Unterschrift einer vertrauenswürdigen Stelle (z.B. DTAG)

  Standard: z.B. X.509

Empfang einer mittels PGP verschlüsselten E-Mail

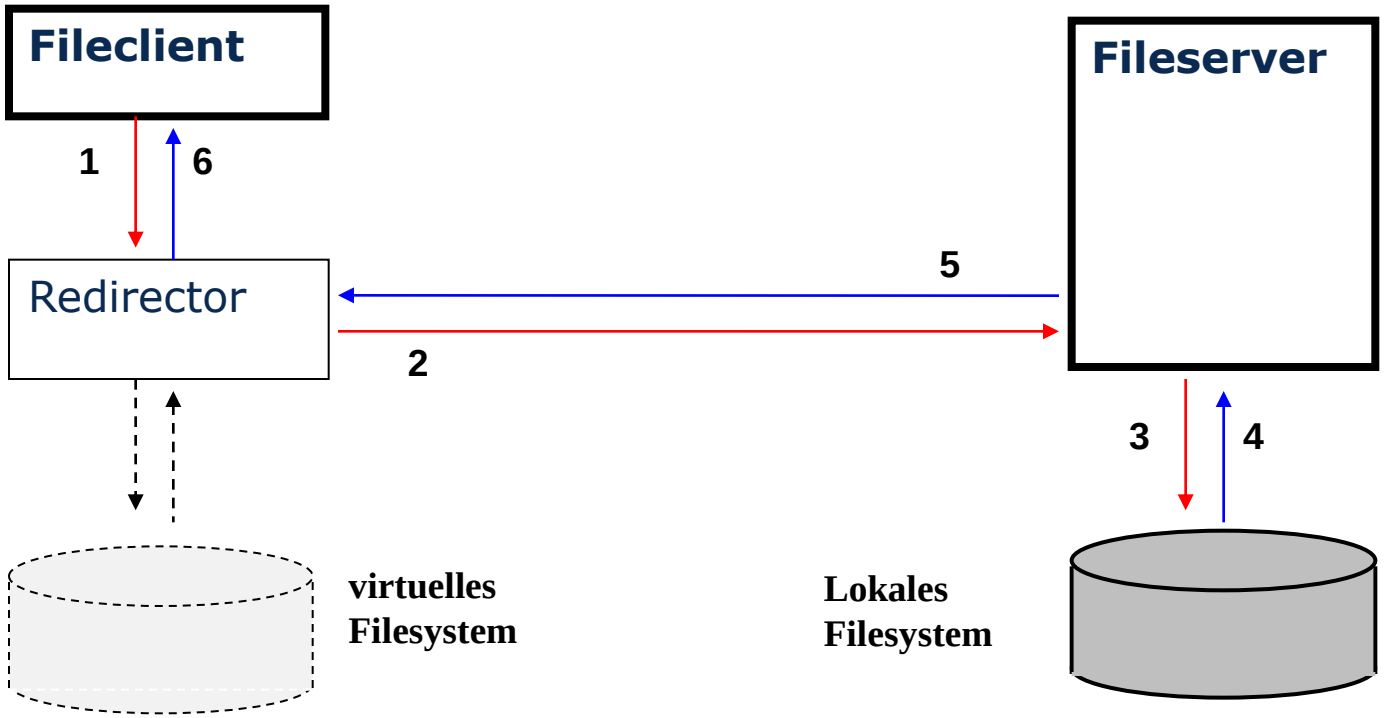


Anzeige der entschlüsselten Nachricht



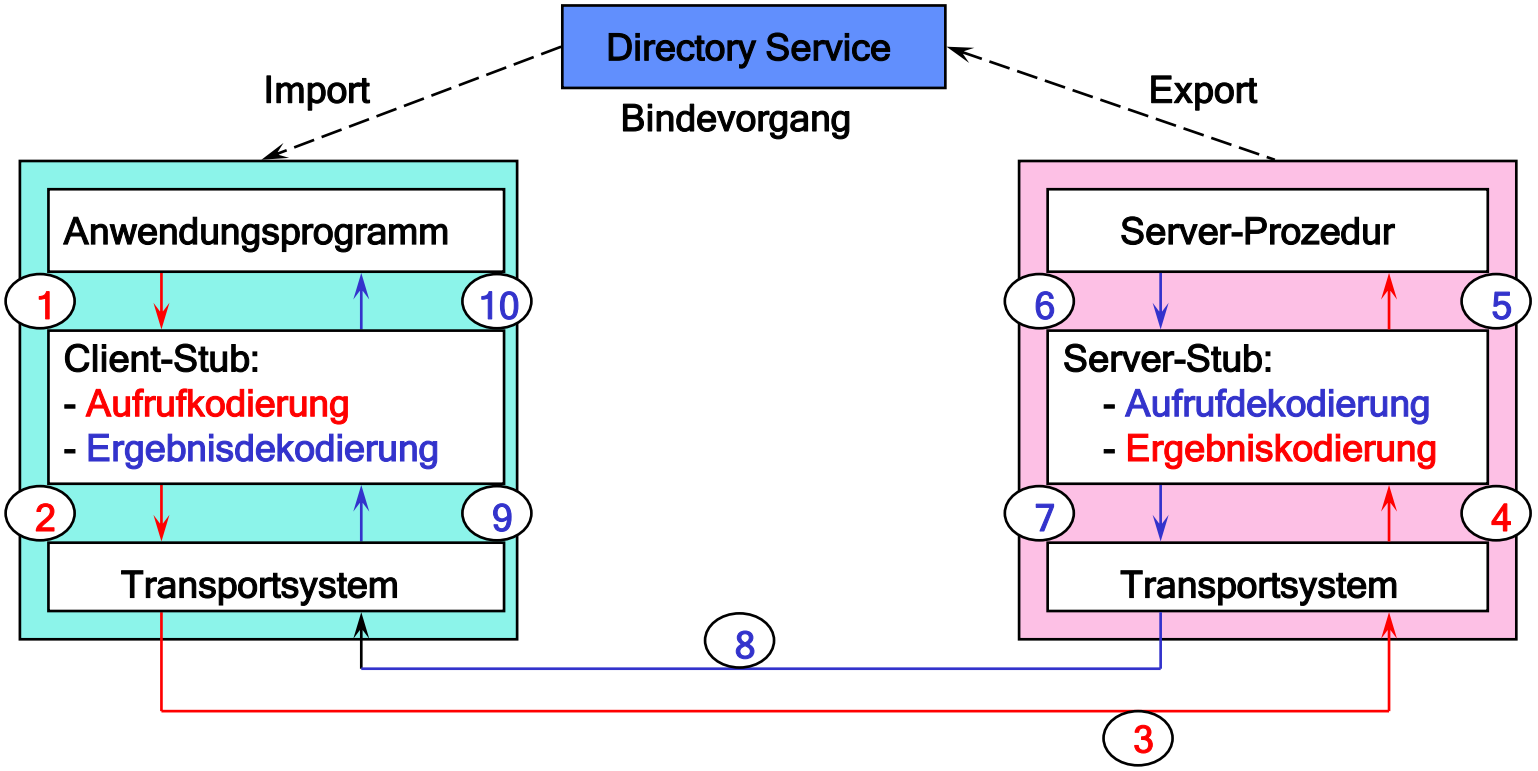
Applikation verteiltes Filesystem

1 – Aufruf einer Prozedur des Dateisystem
2 – Sender aller Input-Parameter an Fileserver-Prozess
3 – lokaler Aufruf einer Prozedur auf Serverrechner
4 – Rückmeldung der Prozedur
5 – Senden der Output-Parameter zum Client-Prozess
6 – transparentes Prozedurende auf Clientrechner



RPC (Remote Procedure CALL)

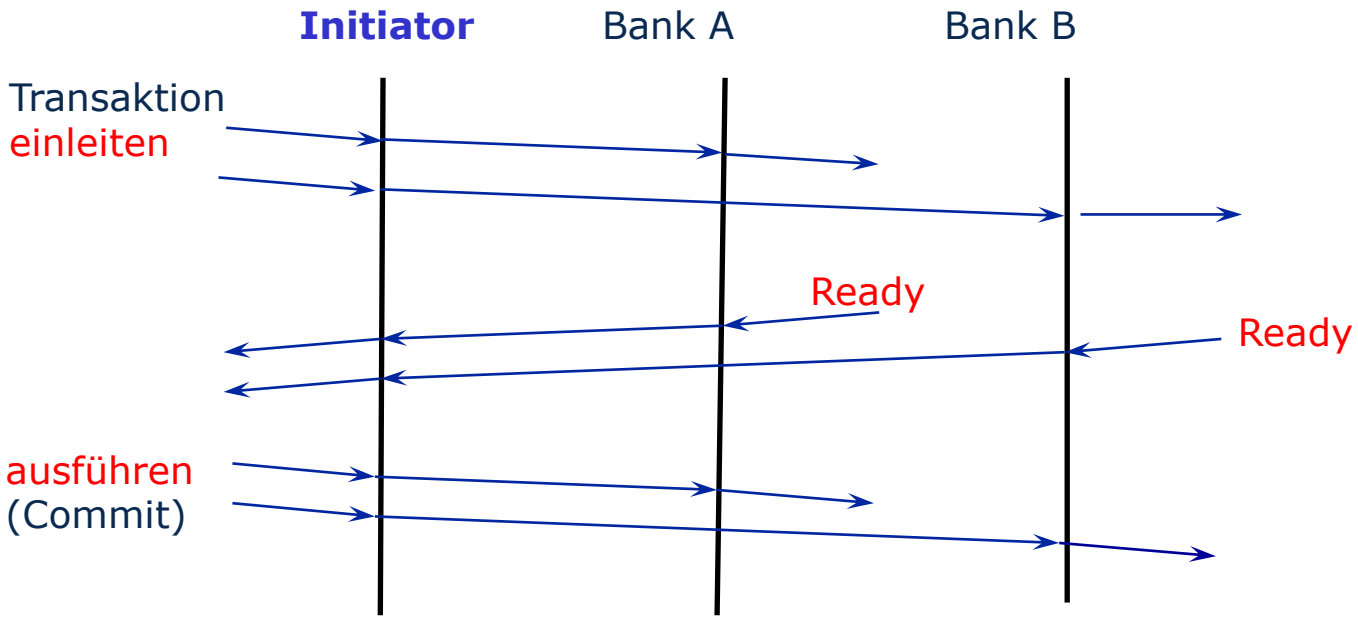
Aufruf beliebiger Prozeduren vom Clientrechner auf einem Serverrechner.



Verteilte Transaktionen

Durchführung atomarer Aktionen "ganz oder gar nicht"
Realisierung: 2-Phasen-Commit-Protokoll

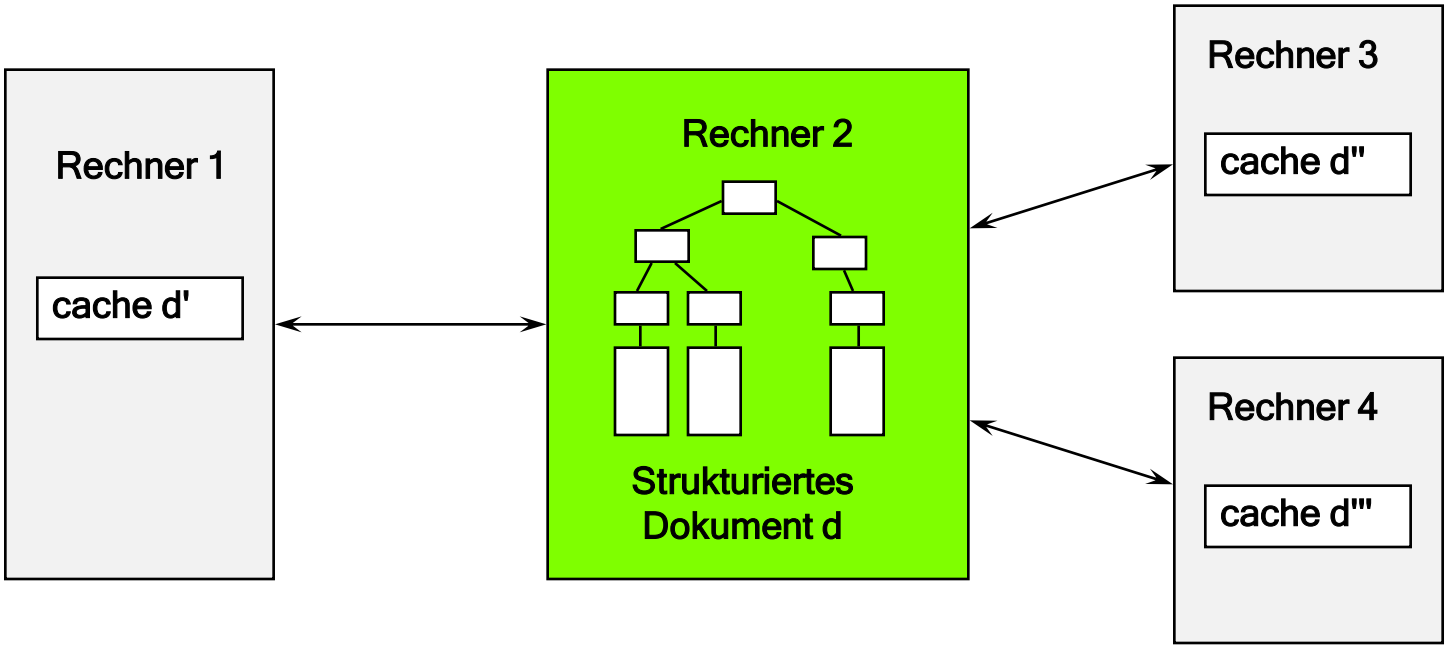
Beispiel: Zahlungstransfer von Bank A nach Bank B



Fehlerfall: Abbruch der Transaktion

Gemeinsamer Dokumentzugriff

- Dokumentlokalisierung über Directory Service
- Zugriff über systemweit eindeutige Dokumentidentifikatoren
- Nebenläufigkeitskontrolle



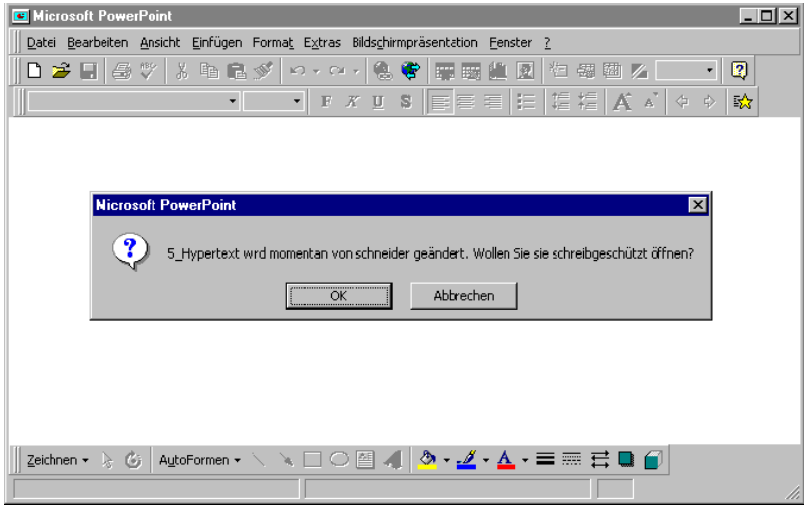
Nebenläufigkeitskontrolle (Konsistenzsicherung)

(Zeit-)paralleler Zugriff auf dieselben Daten durch mehrere Prozesse

- Prozesse lesen Daten,
- arbeiten mit Kopien, — u.U. mehrere Kopien in Umlauf mit unterschiedlichen Inhalten
- schreiben Änderungen zurück — → evtl. Verletzung der Datenkonsistenz

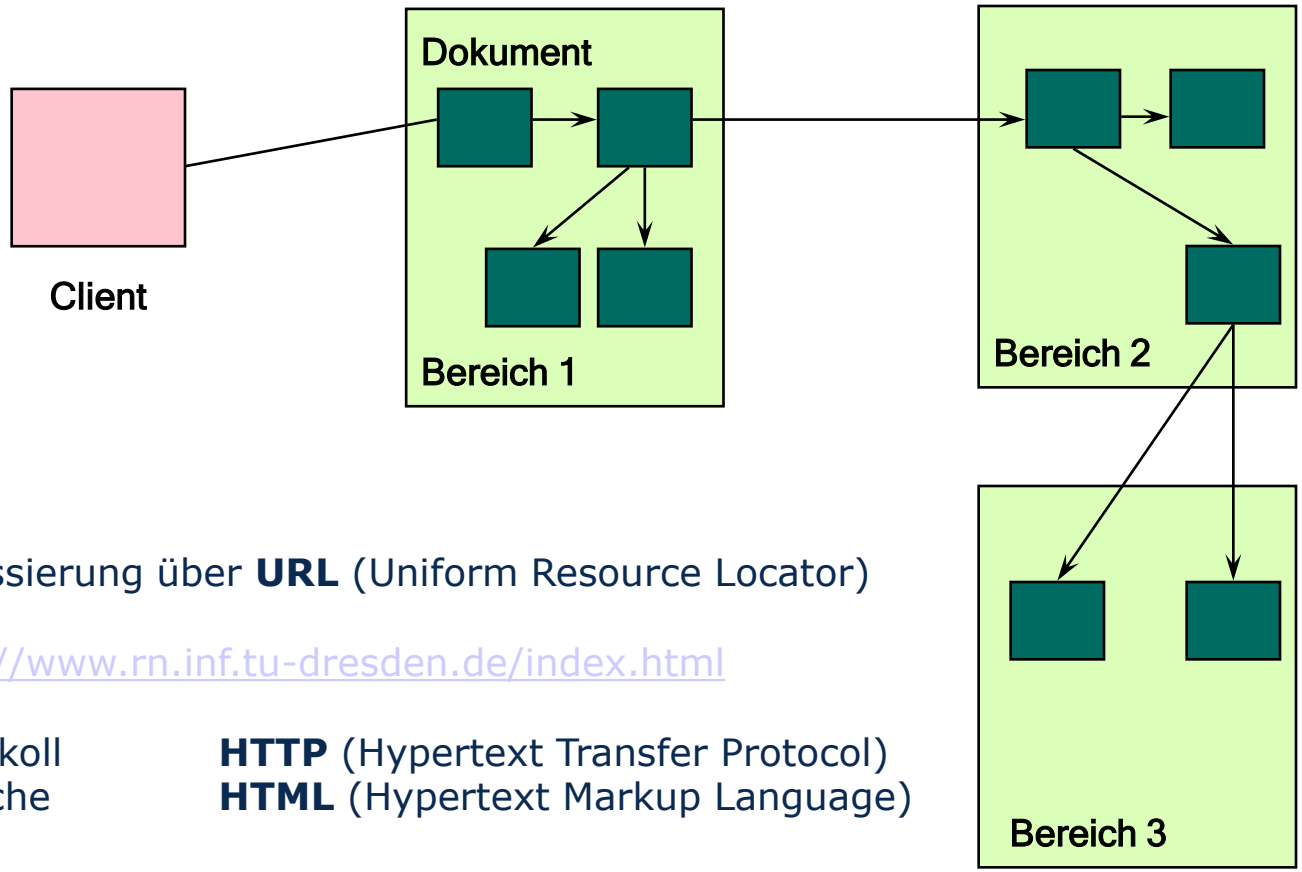
→**temporäre Zugriffssperren**

erforderlich



WWW (World Wide Web)

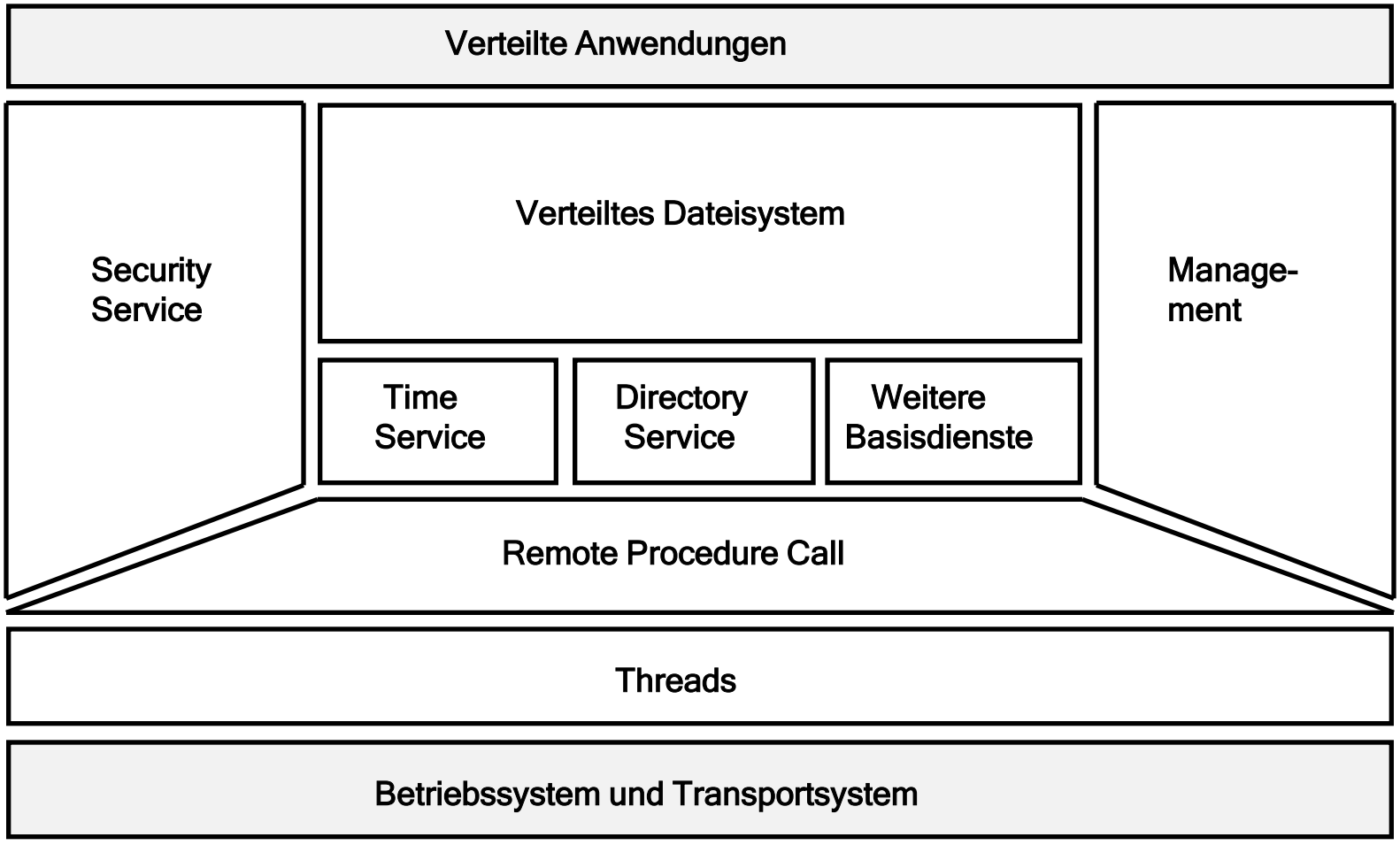
Weltweites Hypertext-System (verlinkte Dokumente)
auf Basis des Internet



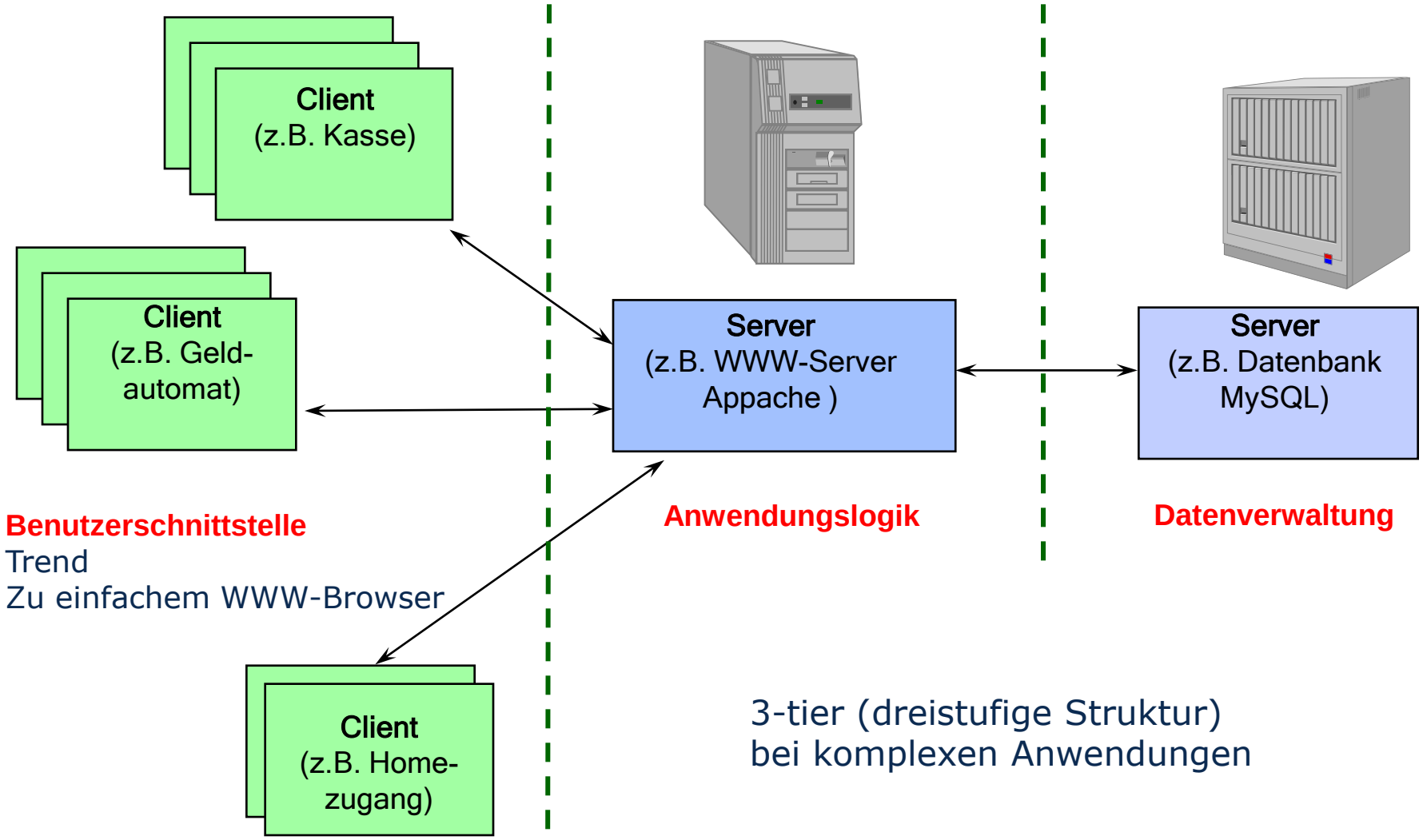
Adressierung über **URL** (Uniform Resource Locator)
z.B.
http://www.rn.inf.tu-dresden.de/index.html

Protokoll	**HTTP** (Hypertext Transfer Protocol)
Sprache	**HTML** (Hypertext Markup Language)

Entwicklungsumgebungen



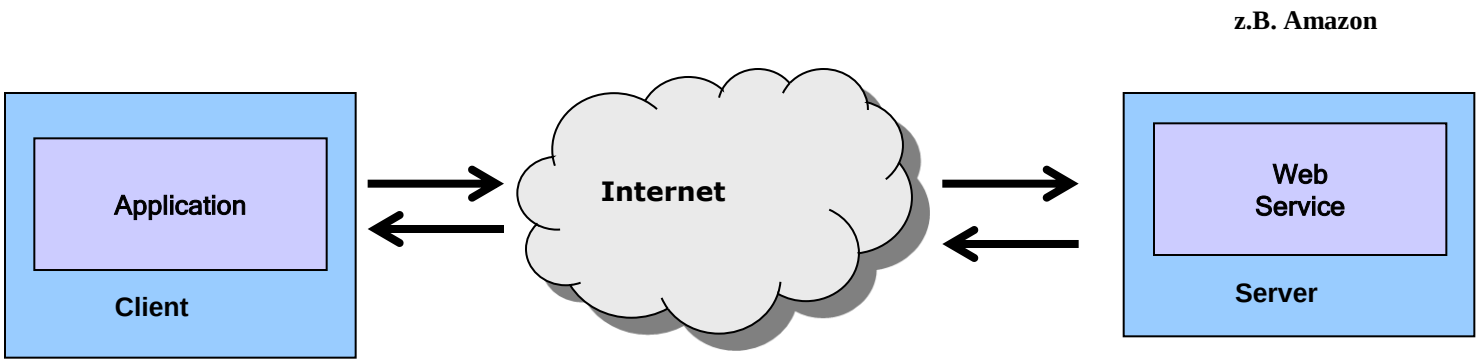
Mehrstufige Architekturen



Webservices

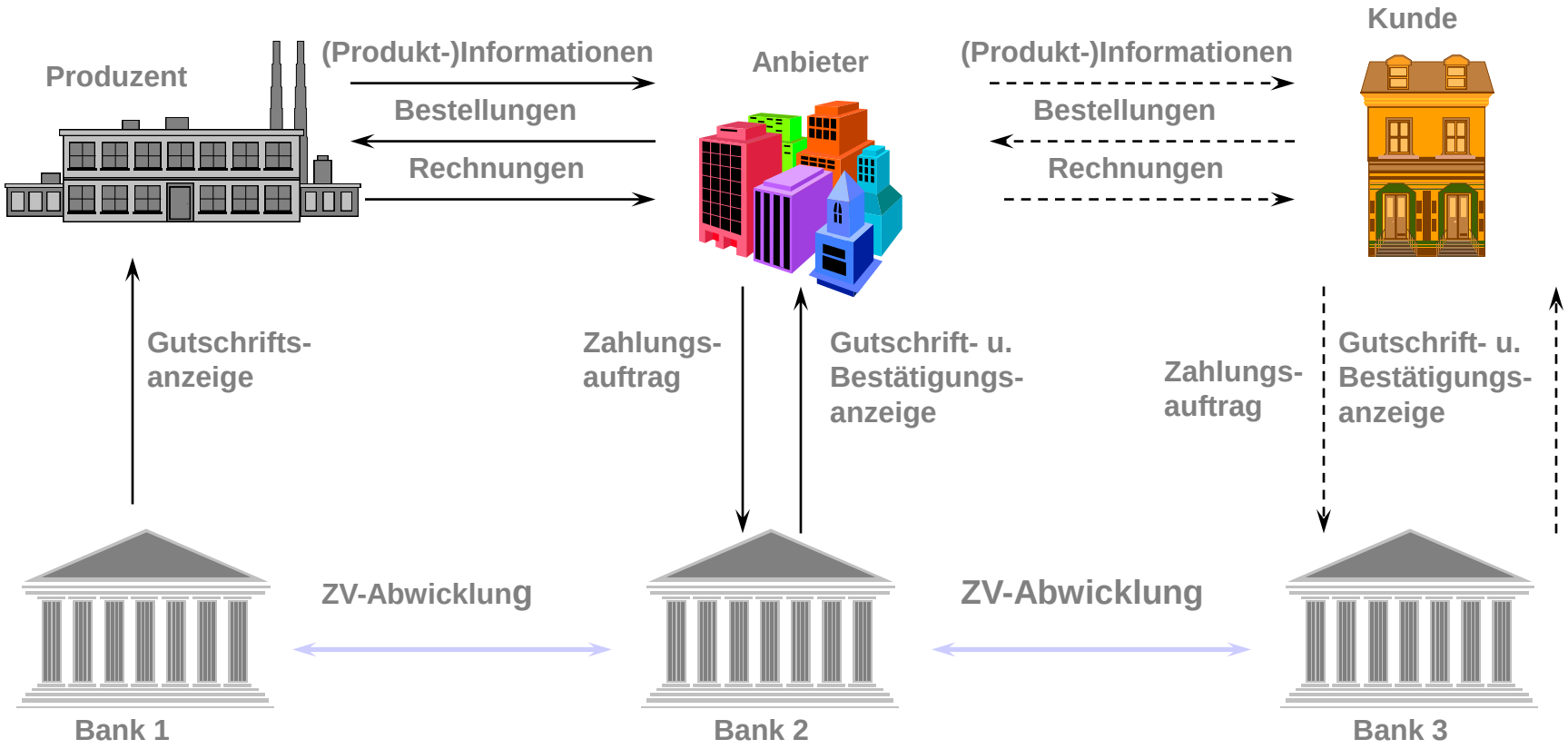
Dienstleistungen,
die über das Internet bereitgestellt werden

- Übertragungsprotokoll meist HTTP
  dadurch leichte Firewall-Durchdringung
- Parameter für Aufruf und Antwort in XML kodiert.
- Adressierung der Webservices über URI



Elektronische Märkte

Weltweite Durchdringung aller Bereiche



Möglichkeiten und Gefahren

Vollautomatische Abläufe

- z.B. Fahren ohne Lokführer + kein menschliches Versagen
  - ???

Wettbewerb/Monopolisierung

- z.B. Dominanz weniger Firmen

Freiheit des Internet, z.B.

- z.B. Missbrauch, aber auch Zensur

Soziales Leben

- z.B. Krankenpflege