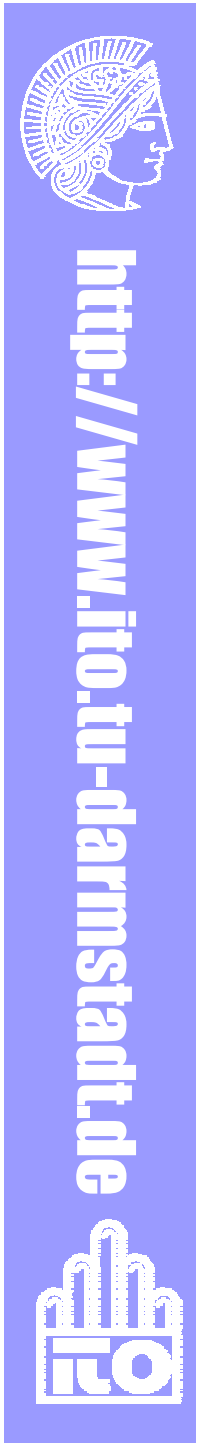
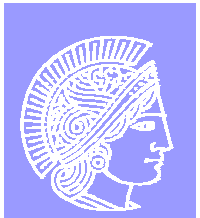
Situationsabhängige Zugriffskontrolle in Smart Environments

Ralf Steinmetz &
Max Mühlhäuser

ITO - IT Transfer Office
TU Darmstadt

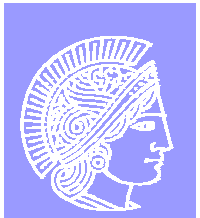


Einführung



- Fakt: Mobilität
- Trends
  - Handy-Boom
  - Drahtlose Vernetzung (GPRS, UMTS, Wireless LAN, Bluetooth, …)
  - Chipkarten (Versichertenkarte, Handy-SIM, Geldkarte, Kreditkarte, …)
  - Heterogenität & Konvergenz
- PDA als visible/demo Computing

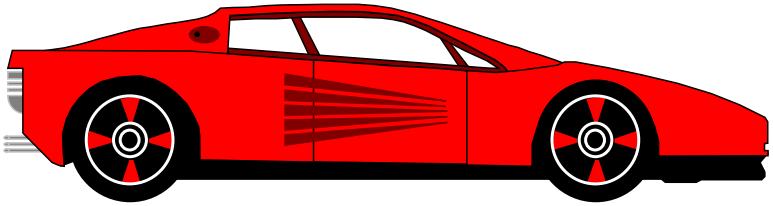
Einführung



- Intelligentes Handy/PDA werden ubiquitär sein
- Verschiedene Funktionalitäten werden auf einer Chipkarte/einem PDA vereinigt sein
- Drahtlose Netzwerke werden überall sein
  - unterschiedliche Technologien
  - verschiedene Betreiber (Netzprovider, Firmen, Privatpersonen)
  - unterschiedliche Reichweite

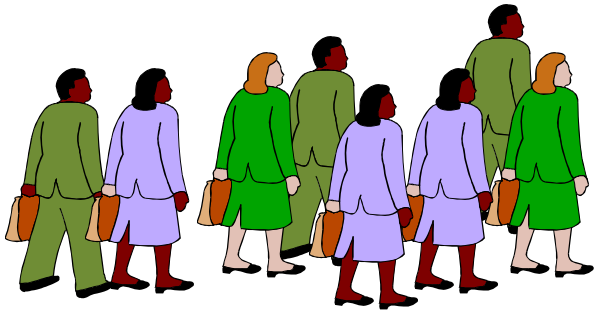
Szenarien

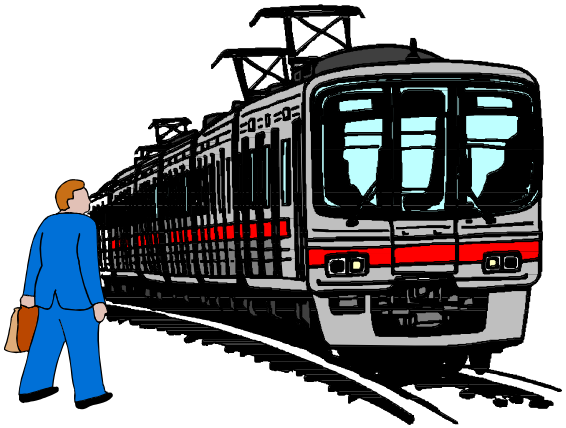
- Parkhaus:
  - Parkbeginn wird registriert und Benutzer zugeordnet
  - bei Verlassen Abuchung der Parkgebühren
  - freier Platz wird zugewiesen



Szenarien

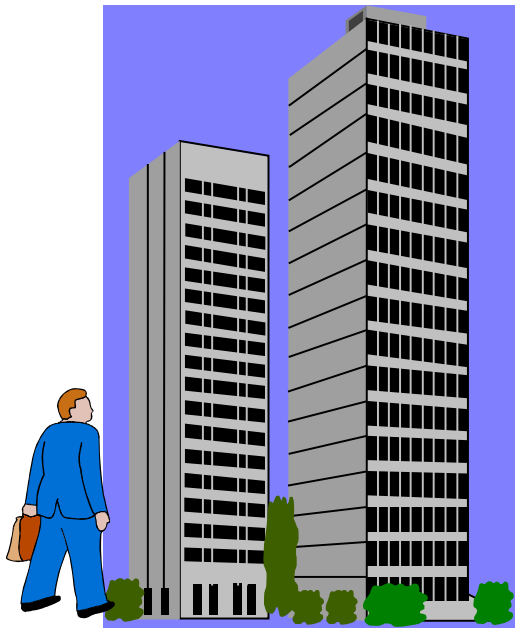
- S-Bahn:
  - PDA informiert über Verspätungen und kennt Abfahrtsort des Zuges
  - Benutzung wird automatisch erfaßt und abgerechnet





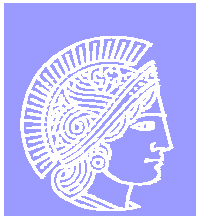
Szenarien

- Firma
  - Einlaß mittles elektronischem Firmenausweis
  - Arbeitsumgebung zieht mit
  - Kollegen können Aufenthaltsort ermitteln
  - Kantinenessen wird erfaßt
  - ...

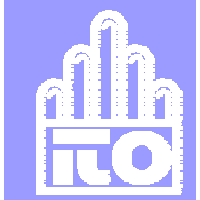


Szenarien: Roomware®

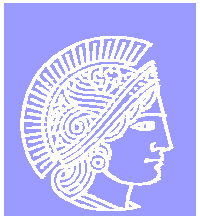
Funktionalität



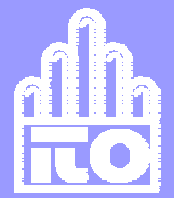
- Heterogenität vs. Universelle Protokolle
- Trennung der Dienste
  - Identifikation von Diensten anhand von Dienstbeschreibungen
- Aushandeln von wirtschaftlichen/rechtlichen Abmachungen
- Technologien
  - zB. Einsatz von Stellvertretern ("Proxies")



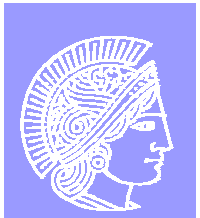
„Funktions“sicherheit



- Ausfallsicherheit der Netze
- Redundanz von Rechnern und PDAs
- Schutz gegen Missbrauch
  - (Viren, Flooding, ...)
- Strikte Trennung der Dienste
- Dienstbeschreibungen
- Robustheit der Dienste
  - bei defekten PDAs/Netzen

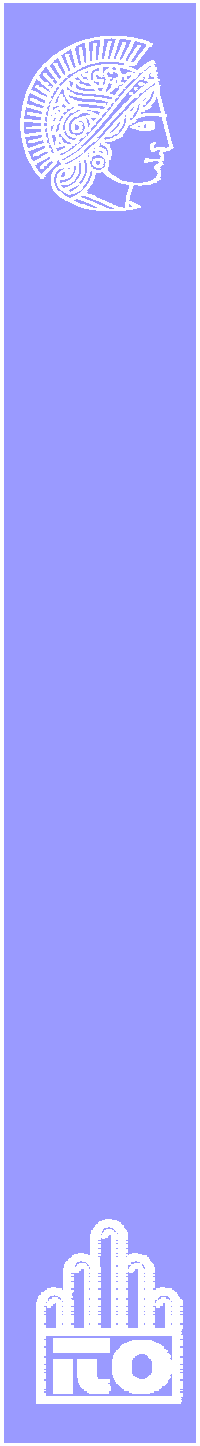


Situated Computing:Umfeld



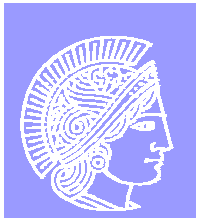
- PDA kann sich durch eigene Lokalisierung an Umfeld anpassen
- Unterschiedliches Recht an verschiedenen Aufenthaltsorten
- PDA muß erkennen/vertrauen, daß sich Funknetz an lokales Recht hält

Informationssicherheit

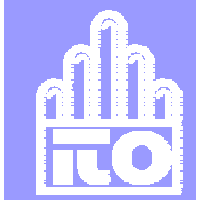


- Zurechenbarkeit
  - Authentifizierung der Benutzer & Netze
- Vertraulichkeit
  - Verschlüsselung
  - Anonymität
- Integrität
- Verlust/Diebstahl des PDA
  - Bewußter Mißbrauch
  - PDA hinterläßt Datenspur, die dem Eigentümer zugerechnet wird
    - aber Einsetzbar zum Wiederauffinden

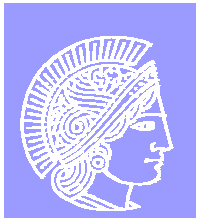
Tracking des Individuums



- Um Dienste in Anspruch zu nehmen, braucht PDA Zugriff auf Netze
- Dazu meldet er sich bei erreichbaren Netzen automatisch an
- Dadurch hinterläßt er Datenspur, die sich (vermutlich) diesem PDA zuordnen läßt
- Aufzeichnung alle Aktivitäten eines Individuums durch Zusammenführung der Zugriffskontrolle erscheint möglich
  - Kontrolle a la „Big Brother“ wird Realität



Tracking eines Ortes



- In gleicher Weise können Personen durch Betreiben eines Funknetzes Informationen über alle Aktivitäten an einem Ort erlangen
- Genauso: mit Hilfe ihres PDAs können Personen Informationen über vorhandene Netzwerke erlangen
  - z.B. kann die Existenz eines Banknetzes interessant sein

Fragestellungen

- Inwieweit läßt sich Anonymität in ubiquitären Netzen erreichen?
  - Da ggf. weniger: Konsequenzen
- Ist es überhaupt sinnvoll, viele (wieviele) Funktionen auf einem Gerät zu vereinigen?
- Ist (wie) Skalierbarkeit der vorgeschlagenen Lösungen möglich?