



# Security Challenges of Location-Aware Mobile Business

---

Emin Islam Tatlı, Dirk Stegemann, Stefan Lucks  
Theoretische Informatik, Universität Mannheim  
März 2005



# Überblick

---

- The Mobile Business Research Group
- Context- und Location-awareness
- Systemarchitektur
- Sicherheitsanforderungen
- Weitere Forschung



# Mobile Business Research Group

---

*Generic platform for context-aware and location-aware mobile business applications*

- Fakultätsübergreifendes Projekt an der Uni Mannheim
- 7 beteiligte Lehrstühle
  - Informatik
  - Wirtschaftsinformatik
  - BWL
- Industriekooperationen mit
  - SAP AG, Walldorf
  - CAS Software AG, Karlsruhe
- Web: <http://www.m-business.uni-mannheim.de/>



# Location und Context

---

Unsere (Arbeits-)Definitionen:

**Context** = Information used to deliver a service which is not explicitly input by the service requestor, but becomes visible during the course of the service delivery (usually in the result).

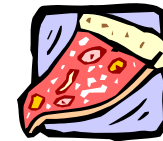
A **Context-aware application** considers context when providing its service.

Wichtige (Kontext)Information: Location des Benutzers

# Beispiele

## ■ Kontextbasierte Gelbe Seiten

- Finde die nächstgelegene Werkstatt meiner Automarke.
- Finde einen Pizzaservice, der mir meine Lieblingspizza für höchstens 8 € innerhalb von 15 Minuten ins Büro liefert.

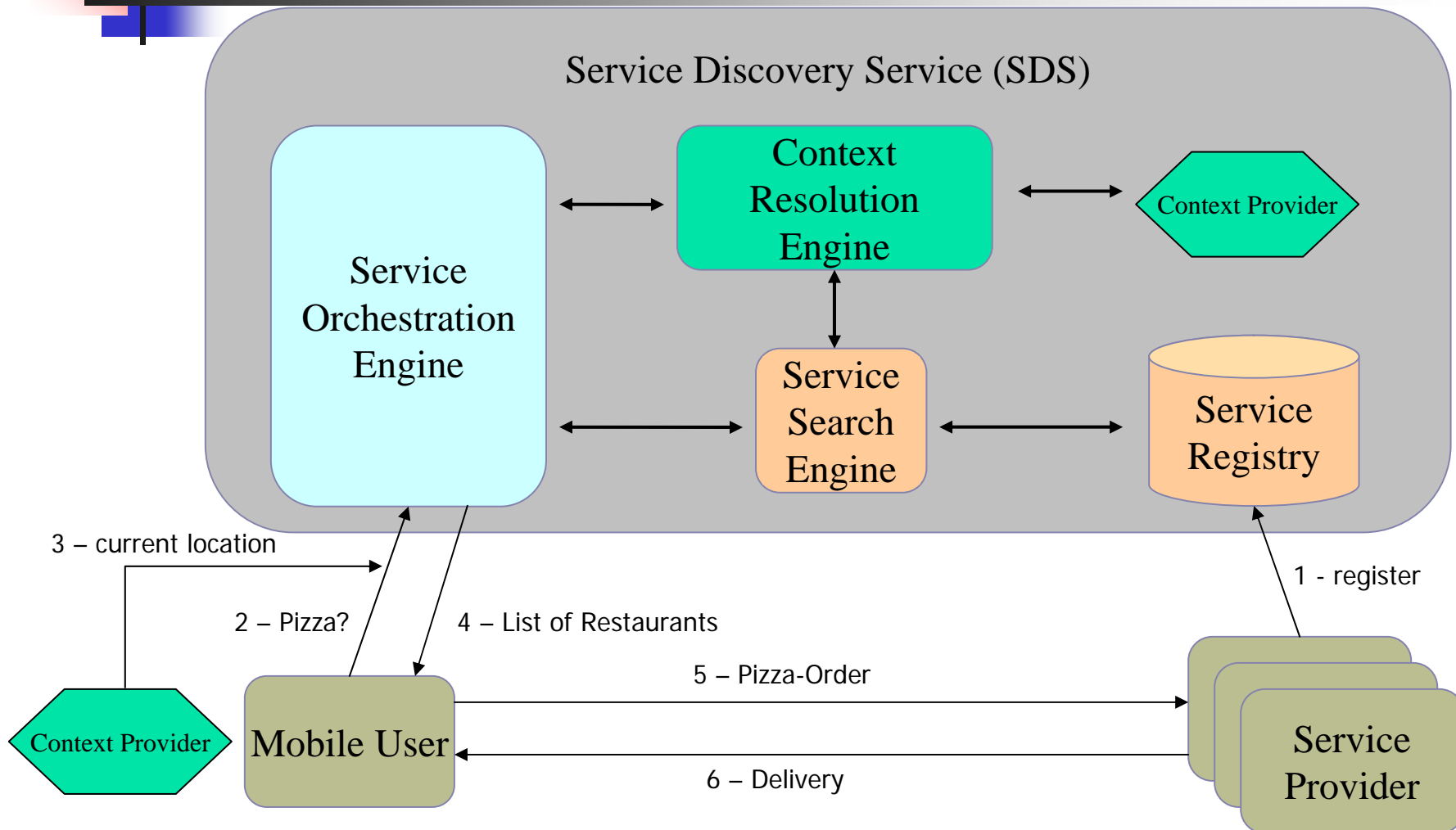


## ■ Kontextbasierte Navigation

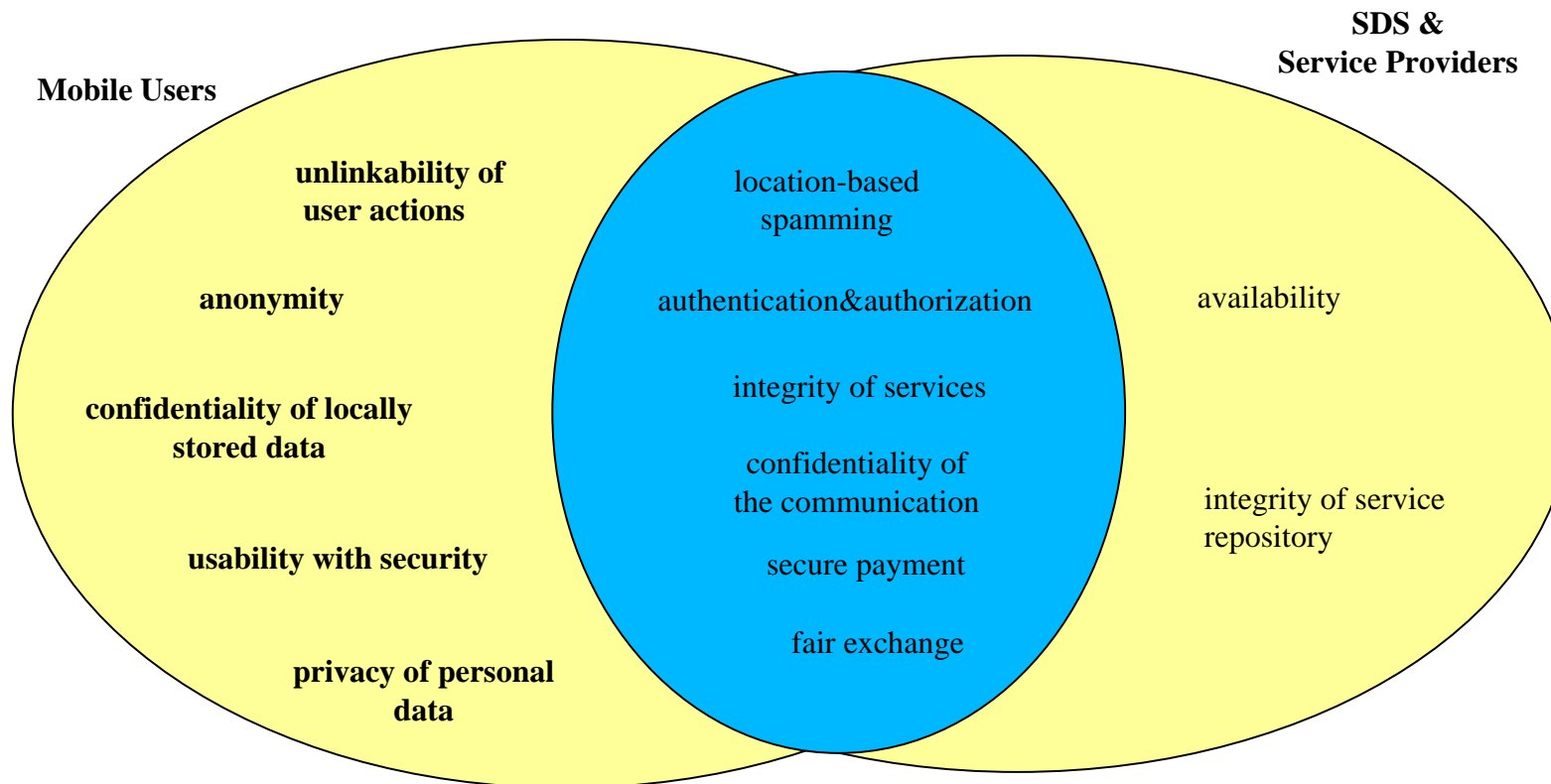
- Navigiere mich und meine Kollegen trockenen Fußes zum nächsten freien Besprechungsraum auf dem Messegelände.



# Systemarchitektur



# Sicherheitsanforderungen





# Anonymität

---

**Anonymität** = Nutzung von Ressourcen ohne Preisgabe der eigenen Identität

Aber: Service Provider brauchen eindeutige Benutzerrepräsentation

*Idee: Benutze Pseudonyme*



# Unlinkability von Pseudonymen

---

**Linkability** von Aktionen A und B =  
*Sind A und B durch denselben Benutzer  
ausgelöst worden?*  
ist entscheidbar.

Linkability von Transaktionen  
+  
Kooperierende Service Provider  
=  
Möglicher Anonymitätsverlust



# Unlinkability von Pseudonymen

---

Andererseits:

Unlinkability von anonymen  
Einzel-Transaktionen

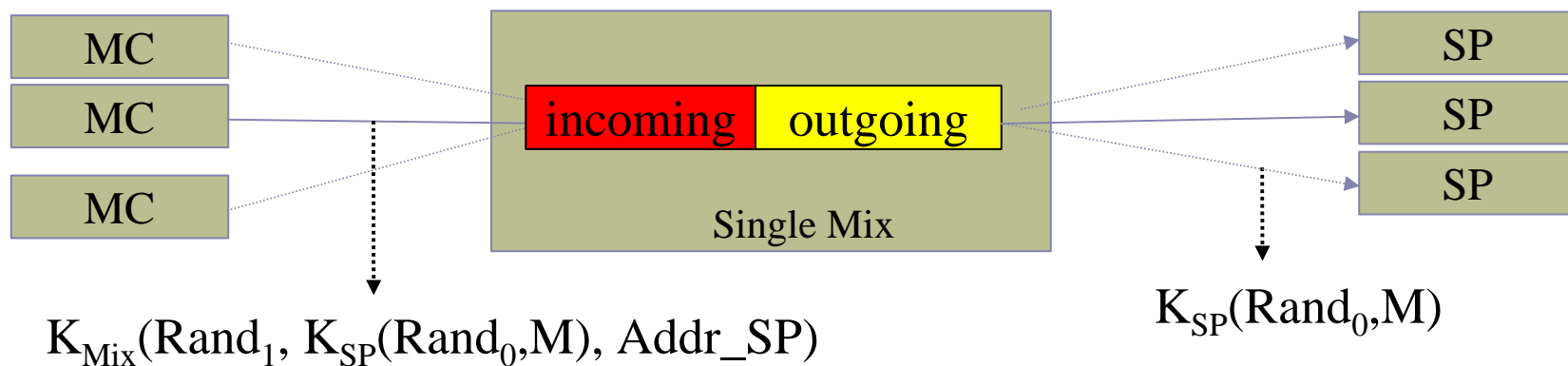


Anonymität sichergestellt

# Unlinkability mit Mixes

Mix:

- Computer zwischen Sender and Empfänger
- Leitet Nachrichten an den Empfänger weiter





# Schutz personenbezogener Daten

---

- Viele Services nur unter Preisgabe persönlicher Informationen (insbes. Location) sinnvoll nutzbar
  - Werkstattfinder: Automarke, Modell, Art des Schadens, ...
  - Pizzaservice: Lieblingspizza, Preisobergrenzen
- Benutzer verlangen explizite Kontrolle über die Weitergabe persönlicher Daten

Mögliche Lösung:

- Identity Manager



# Identity Manager

---

- Benutzerinterface zur
  - Erzeugung von virtuellen IDs
  - Zuordnung von ausgewählten Daten zu jeder ID
- Benutzer kann
  - ID für jede Transaktion individuell auswählen
  - Übertragung persönlicher Daten explizit kontrollieren

# Identity Manager



(vgl. [http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom\\_technik/atus/idm-demo/](http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom_technik/atus/idm-demo/))



# Vertraulichkeit lokal gespeicherter Daten

---

- Diebstahl von mobilen Geräten an der Tagesordnung
- Lokale Daten müssen vor unberechtigtem Zugriff geschützt werden
  - Profilinformationen
  - Passwörter
  - Private Schlüssel

## Mögliche Lösungen:

- Two-factor authentication
- Password-based encryption



# Sicherheit vs. Benutzbarkeit

---

- Oft geht Benutzbarkeit vor Sicherheit:
  - Schwache Passwörter
  - Ignorieren von Warnungen über abgelaufene Zertifikate
- Verschiedene Benutzer und Anwendungen – verschiedene Sicherheitsbedürfnisse

Mögliche Lösung:

- Dynamisch konfigurierbares security policy management system (DPMS)



# Sicherheit vs. Benutzbarkeit

---

Komponenten eines DPMS:

- Password Manager
- Single-Sign-On
- Security Level Manager
- Identity Manager



# Weitere Forschung

---

*Design einer offenen Sicherheitsarchitektur zur  
Integration in das M-Business Application Framework*



# Security Challenges of Location-Aware Mobile Business

---

*Vielen Dank !*

Emin Islam Tatlı, Dirk Stegemann, Stefan Lucks  
Theoretische Informatik, Universität Mannheim

März 2005