Eine Rechteverwaltungs-platform für heutige LBS-Anwendungen

Tobias Kölsch, Marc Wilhelm

PRIME
Privacy and Identity Management for Europe

T · · Mobile · · ·

Überblick

- Problembeschreibung
- Überblick über Architektur
- Implementierungsdetails
- Sicherheitsbewertung
- Ausblick

Problembeschreibung

- Eingeschränkte Möglichkeit der Rechteverwaltung
  - Global Ja / Nein
- Rechteverwaltung aufwändig
  - Medienbruch
  - SMS / Webseite
- Datenschutz per Vertrag
  - Kontrolle liegt bei Dienstanbieter
  - Unterschiedliche Rechtsauffassung → fragliche Dienste
- Nutzeridentität wird preisgegeben

Problembeschreibung

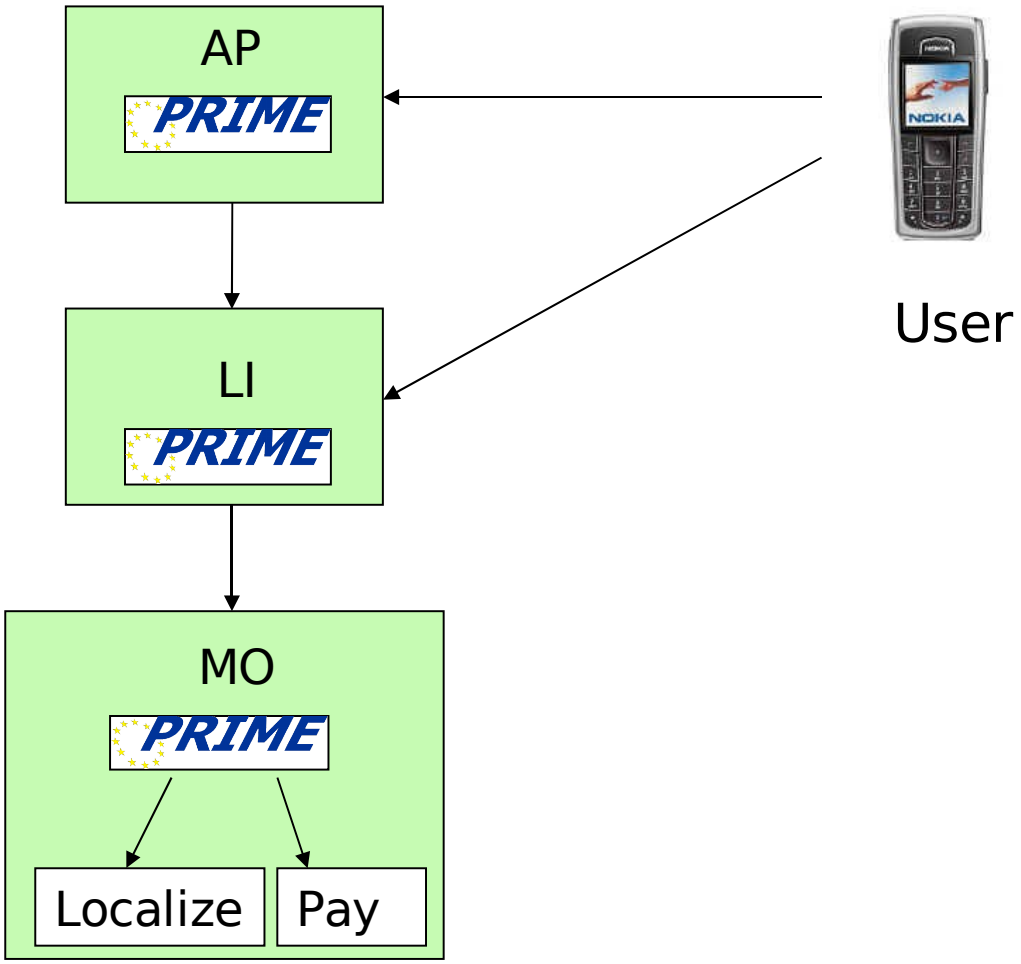
- Problem: Einführung radikal neuer technologien in Telko-Umfeld schwierig
  - Benutzer mit konventioneller Technik
  - Rekonfiguration von Geräten aufwändig
  - Möglichst homogene Infrastruktur erwünscht
  - Große Marktpenetration erwünscht
- Lösung: Hybrider Ansatz
  - Low-Tech-Zugang auf herkömlicher Technik
  - Spezieller Zugang für neue Endgeräte

Pharmacy Search Architektur

Dienstanbieter
- Pharmacy Search -

Ortsdatenmittler

Mobilfunkbetreiber



Akteure

Benutzer
- Einfaches Handy mit WAP Browser

Dienstanbieter AP (Pharmacy Search)
- PRIME funktionalität
- Bietet Apothekensuche an (Pull Dienst)

Ortsdatenmittler LI
- PRIME funktionalität
- Handhabt Rechteverwaltung für den Benutzer
- Vermittelt Ortsdaten und Bezahlung
- Verwaltet Konto des AP
- Teil des MO (rechtliche Gründe)

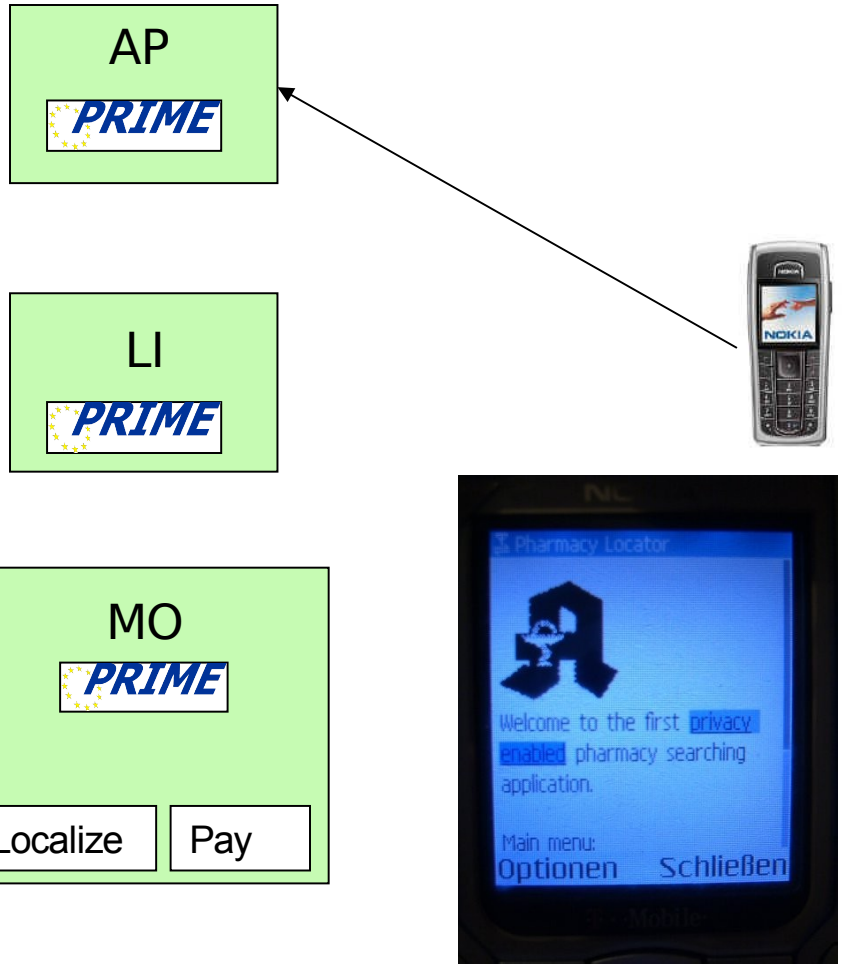
Mobilfunkbetreiber MO
- PRIME funktionalität
- Verwaltet Benutzerkonto
- Bietet Ortsdaten und Kommunikation

PRIME

- IST Projekt des 6. Rahmenprogramm
- 20 Partner aus Akademia und Industrie
- Projekt zur Erstellung eines Nutzerzentrierten IDM
- Ganzheitlicher Ansatz

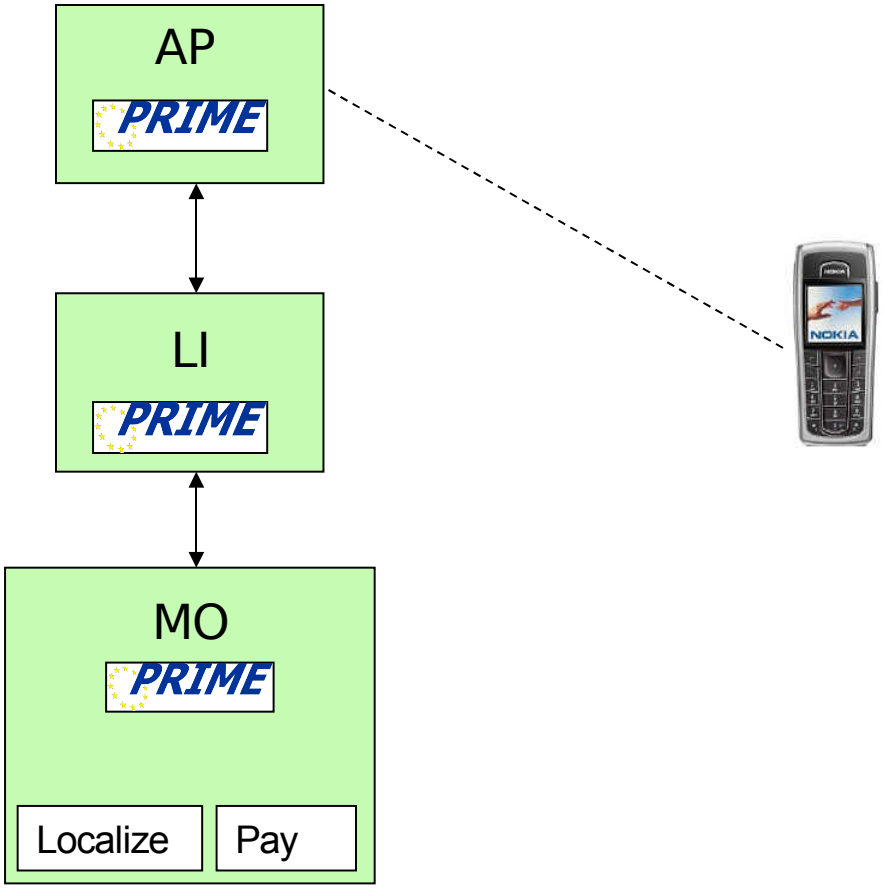
Use Case (Step 1)

- **Dienstanfrage durch Benutzer**



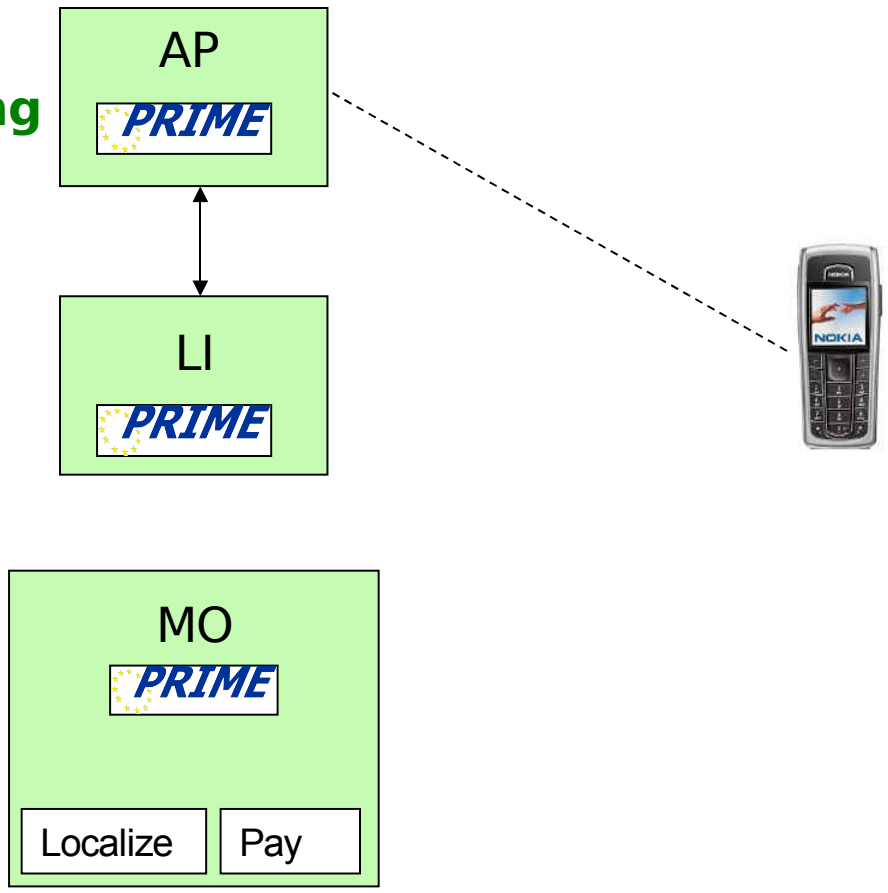
Use Case (Step 2)

- Dienstanfrage durch Benutzer
- **AP erfragt Sitzungs ID mit IP**
  - LI erfragt Benutzer ID
  - MO löst Benutzer ID auf
  - LI übermittelt Sitzungs ID



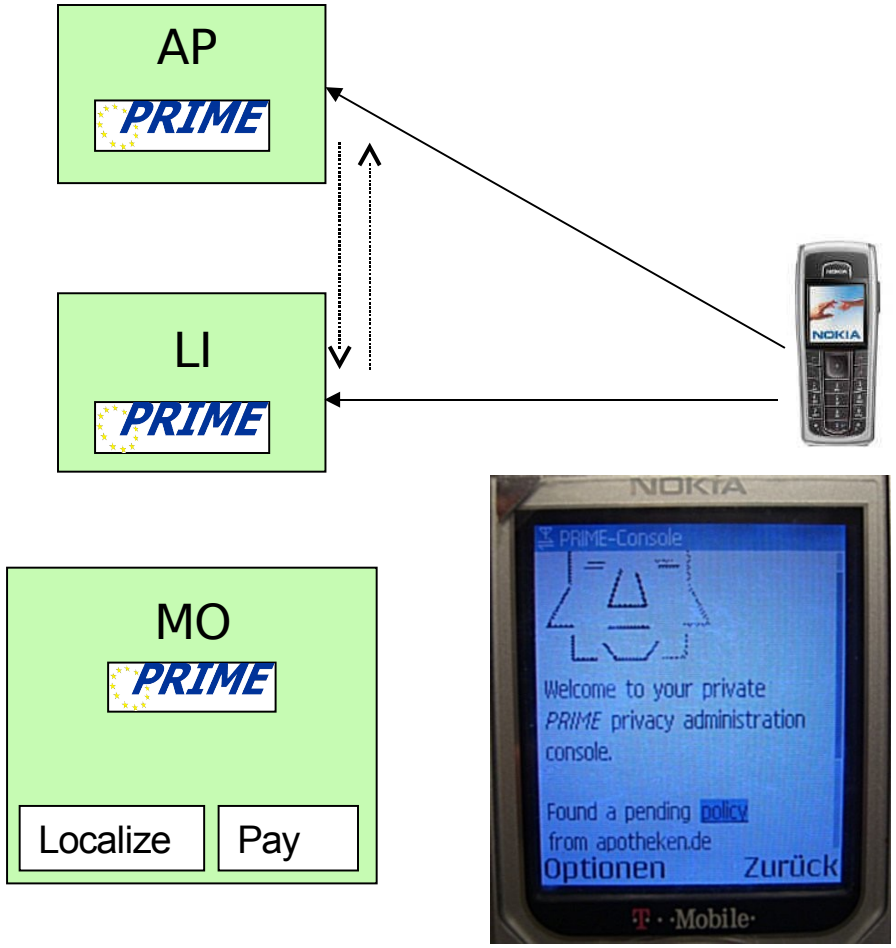
Use Case (Step 3)

- Dienstanfrage durch Benutzer
- AP erfragt Sitzungs ID mit IP
- **AP erfragt Ortsdate & Bezahlung**
  - LI's prüft Zugriffsrecht



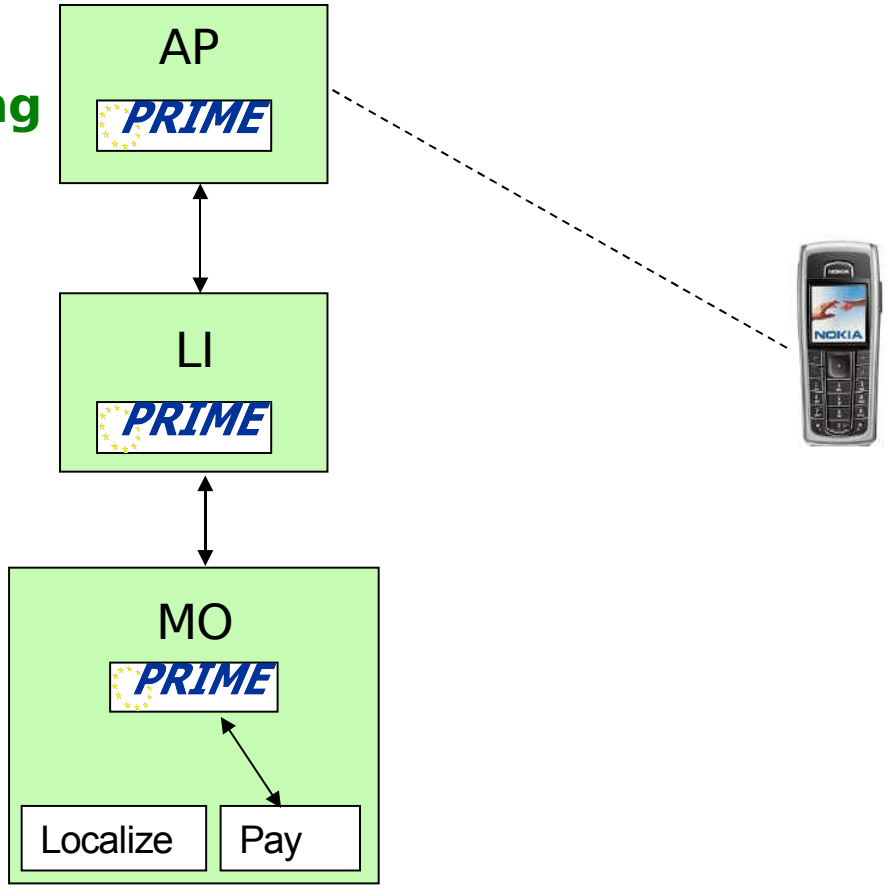
Use Case (Step 4)

- Dienstanfrage durch Benutzer
- AP erfragt Sitzungs ID mit IP
- AP erfragt Ortsdate & Bezahlung
  - LI's prüft Zugriffsrecht
  - **Falls negativ:**
  - AP sendet Berechtigungsvor-schlag an LI
  - AP leitet Benutzer auf LI um
  - Benutzer kann Vorschlag annehmen
  - Benutzer wird zum AP geleitet und Dienst gleich gestartet



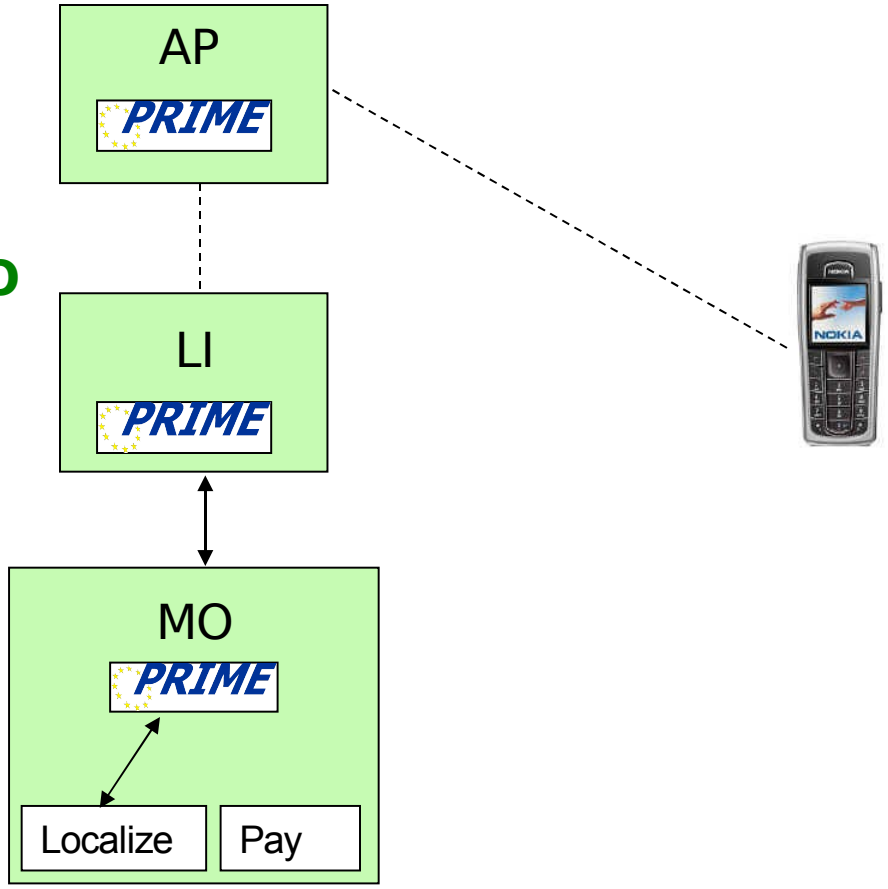
Use Case (Step 5)

- Dienstanfrage durch Benutzer
- **AP erfragt Sitzungs ID mit IP**
- **AP erfragt Ortsdate & Bezahlung**
  - **LI's prüft Zugriffsrecht**
  - **LI reserviert Betrag MO**



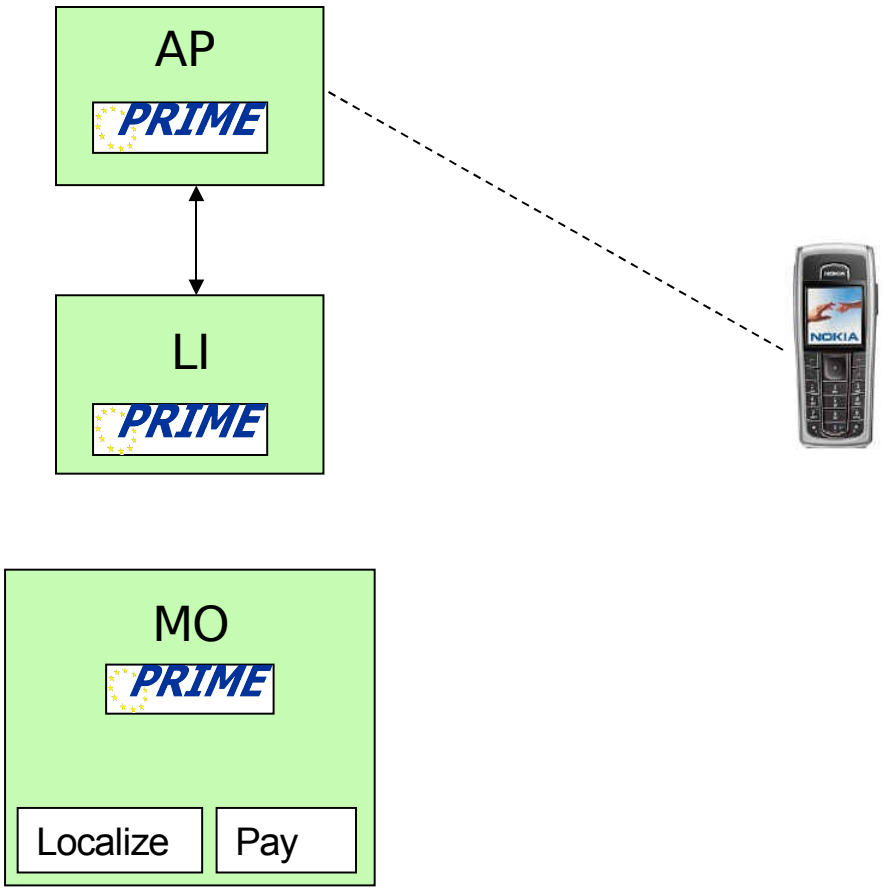
Use Case (Step 6)

- Dienstanfrage durch Benutzer
- AP erfragt Sitzungs ID mit IP
- AP erfragt Ortsdate & Bezahlung
  - LI's prüft Zugriffsrecht
  - LI reserviert Betrag MO
  - **LI erfragt Ortsdaten von MO**



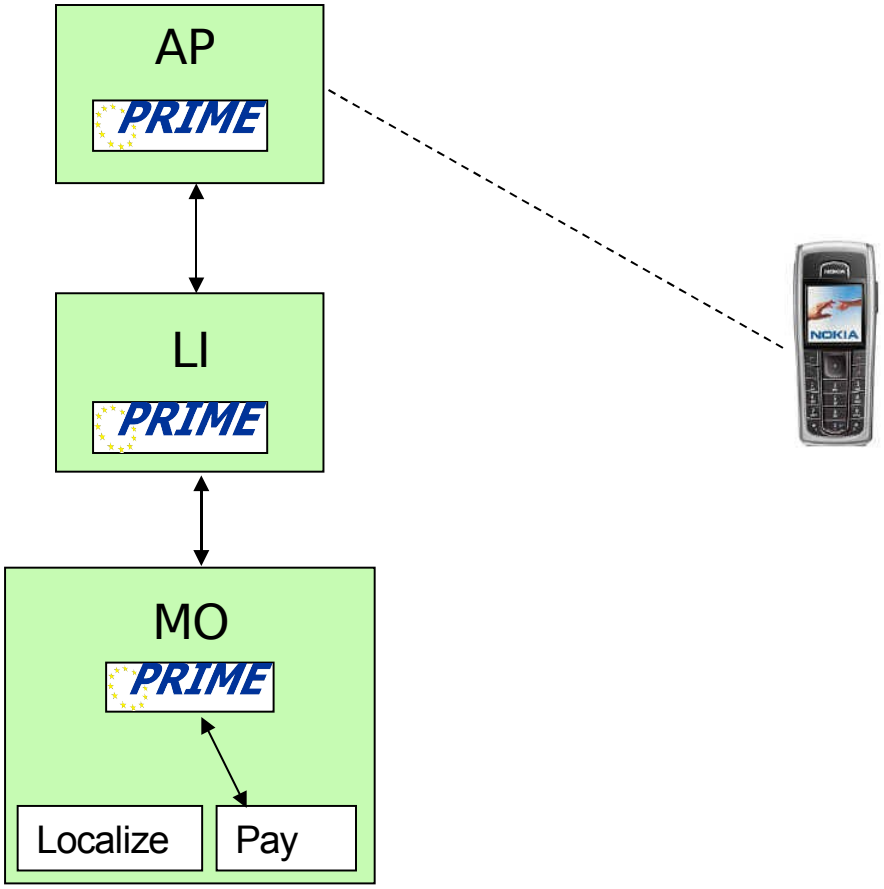
Use Case (Step 7)

- Dienstanfrage durch Benutzer
- AP erfragt Sitzungs ID mit IP
- AP erfragt Ortsdate & Bezahlung
  - LI's prüft Zugriffsrecht
  - LI reserviert Betrag MO
  - LI erfragt Ortsdaten von MO
  - **LI leitet Ortsdaten und Zahlungsreservierung an AP**



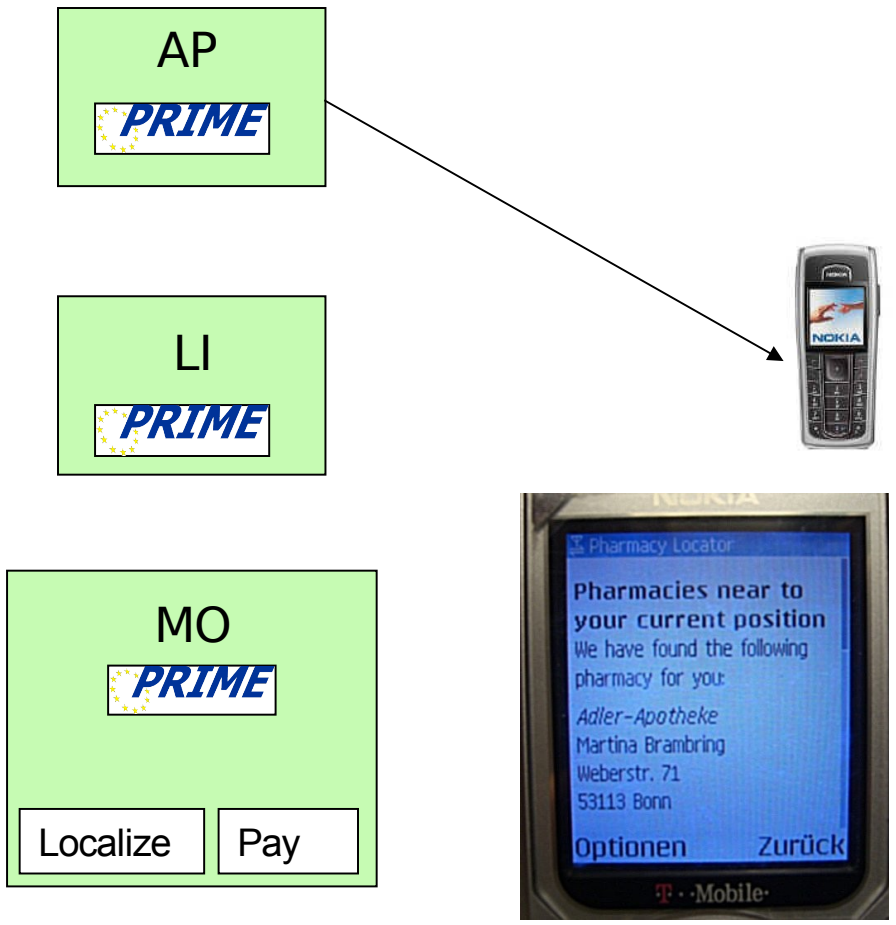
Use Case (Step 8)

- Dienstanfrage durch Benutzer
- AP erfragt Sitzungs ID mit IP
- AP erfragt Ortsdate & Bezahlung
- **AP berechnet Ergebnis**
- **AP führt Bezahlung durch**
  - LI leitet Bezahlung an MO
  - MO bucht und bestätigt
  - LI bucht Lokalisierungskosten und bestätigt



Use Case (Step 9)

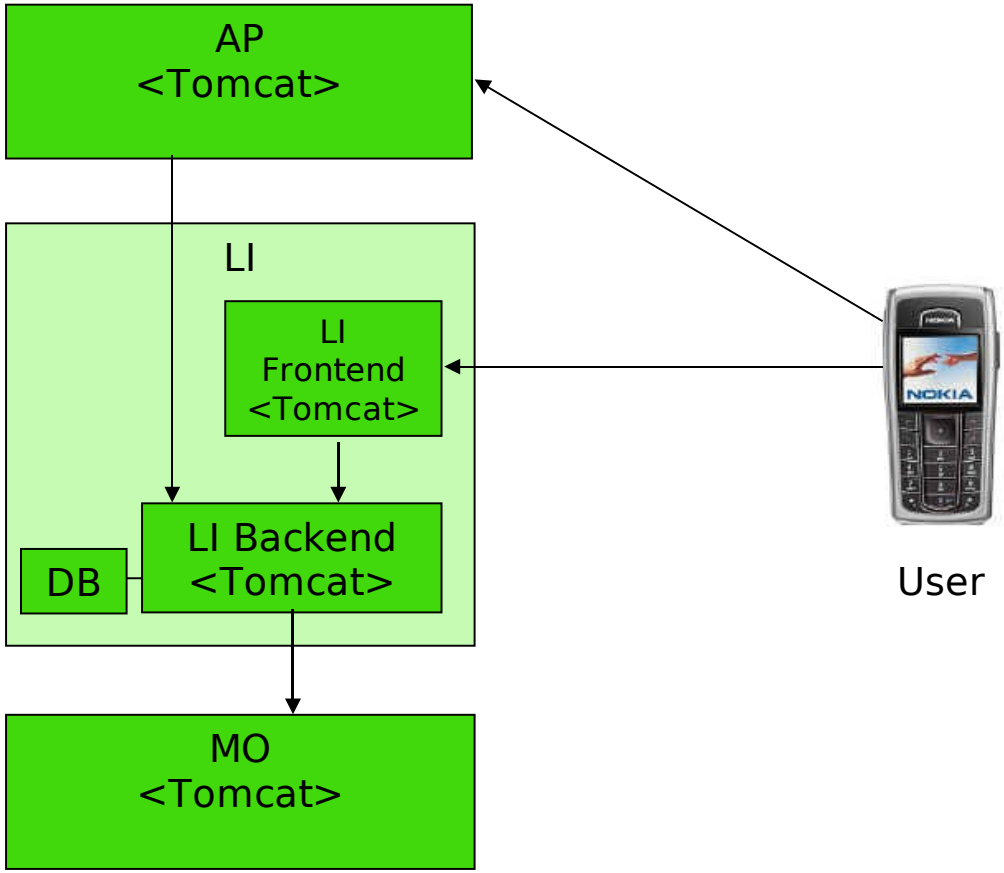
- Dienstanfrage durch Benutzer
- AP erfragt Sitzungs ID mit IP
- AP erfragt Ortsdate & Bezahlung
- AP berechnet Ergebnis
- AP führt Bezahlung durch
- **AP überträgt Ergebnis**



Konsolenfunktionen

Schnell-Zustimmung	Manuelle Einstellung	Protokolleinsicht
		

Instanzen


AP
<Tomcat>
LI
LI
Frontend
<Tomcat>
LI Backend
<Tomcat>
DB
MO
<Tomcat>
NOKIA
User

Technologien

- Tomcat Servlet Container
- MyFaces
- The Spring Framework (Remoting)
- Hibernate
- Maven

Bewertung: Datenfluss

Dienstanbieter	Ortsdatenmittler	Mobilfunkbetreiber
•Temp. Benutzerpseudonym (IP) •Benutzerposition •MO •LI •Benutzer Zahlungsunfähig •Eigenen Zugriffsrechte •Benutzerinteresse an Dienst •Zugriffszeit •Eingeschränktes Surfprofil •HTTP header ○Handy-Modell ○Sprache	•ID des MO •ID des AP •**Permanentes Benutzerpseudonym** •Benutzer IP •**Dienstnutzungsprofil** •Zugriffszeit •**Benutzerposition** •Benutzer Zahlungsunfähigkeit •Benutzereinstellungen •Eingeschränktes Surfprofil •HTTP header ○Handy-Modell ○Sprache	•ID des LI •**Vertragsdaten des Benutzers** •Benutzerposition •Ortungszeit •Benutzer IP •Benutzerkonto

Ausblick

- Erweiterung auf Pull-Szenarien
  - Erhöhung der Einstellmöglichkeiten
  - Anomalieerkennung mit automatischer Benachrichtigung
- Erhöhung des Datenchutzes, 2 Ansätze:
  - Erhöhungung der Erreichbarkeit
    - zusätzliche Schnittstellen
  - Erhöhung des Schutzes (neue Technologien)
    - Mehr Logik beim Mittler
    - Mehr Kontrolle beim Benutzer
    - Erweiterte / spezielle Protokolle

Fragen?