



Präsentation AW1

Sicherheit in Location-based Services durch Zugriffskontrolle

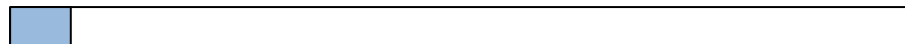
Thomas Schmidt

Hamburg, 08. Juni 2006



Gliederung

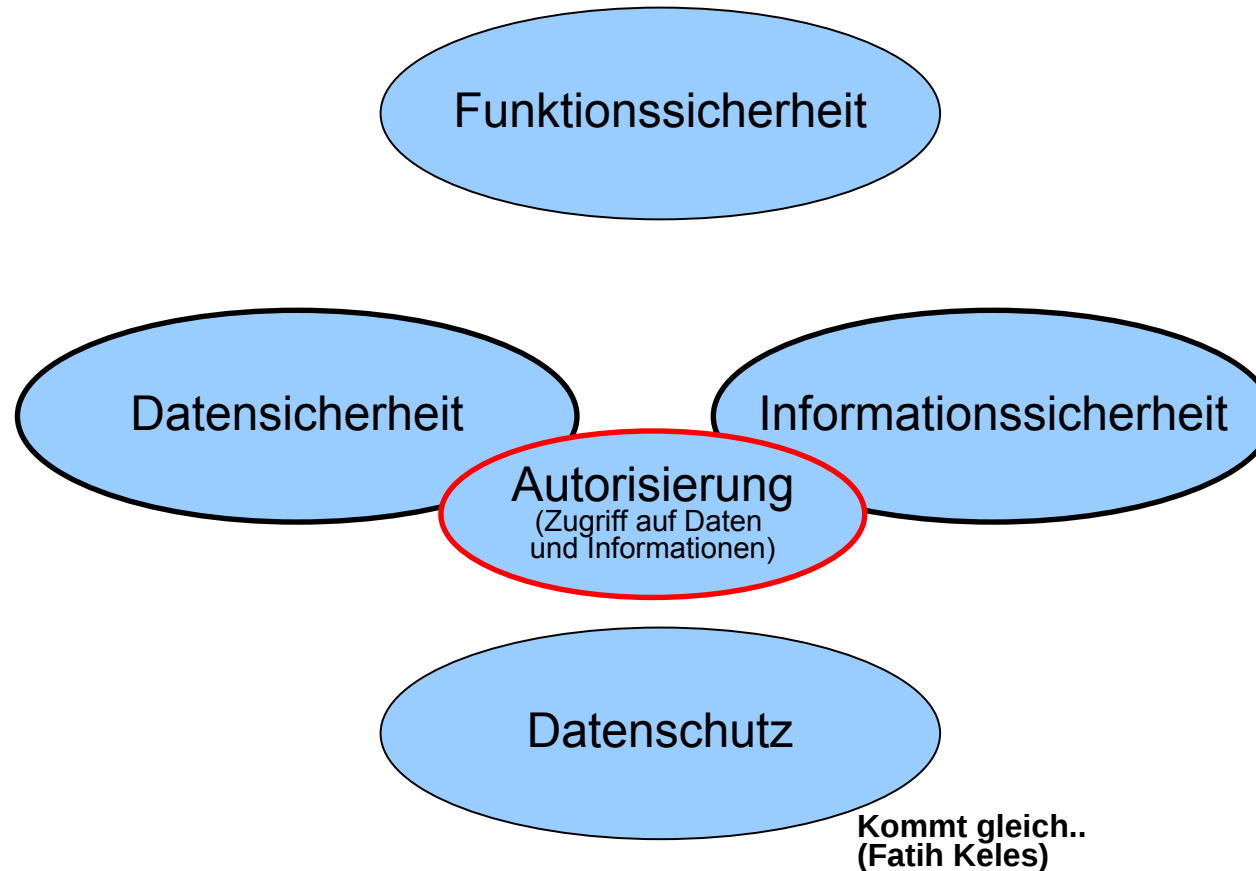
- Motivation
- Sicherheit
- Location-based Services
- Allgemeine Zugriffskontrollstrategien
- Zugriffskontrollstrategie für LBS
- Framework für mobile Geräte
- Szenario
- Zusammenfassung
- Ausblick (3.Semester)



- Mobile Geräte werden immer leistungsfähiger
- Viele Einsatzmöglichkeiten in Unternehmen
- Durch Mobilität steigt Flexibilität
- Fragen:
 - Entstehen durch Kenntnis des Ortes neue Sicherheitsanforderungen?
 - Kann die Sicherheit durch Kenntnis des Ortes verbessert werden?

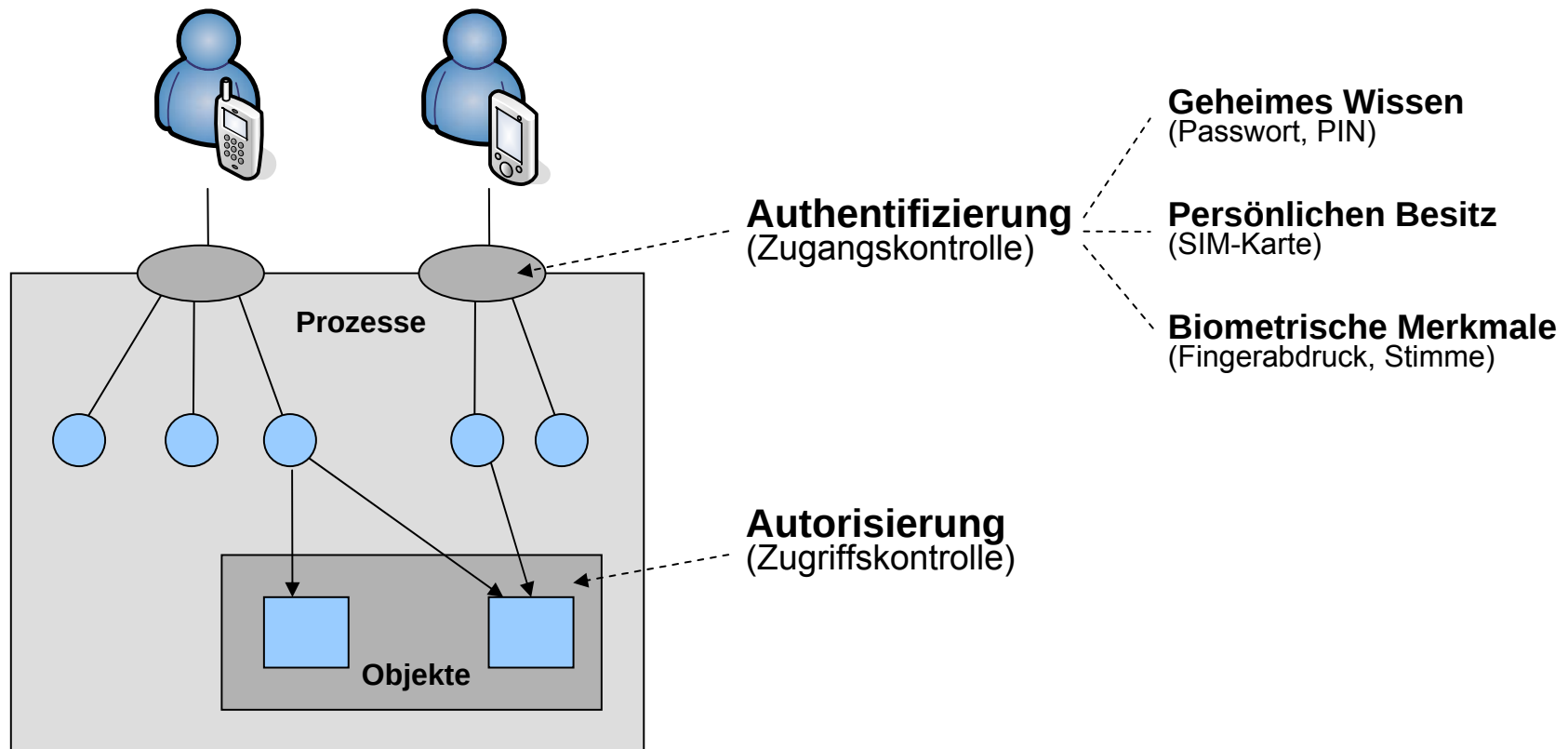


Sicherheit



[Eckert2001]

Sicherheit

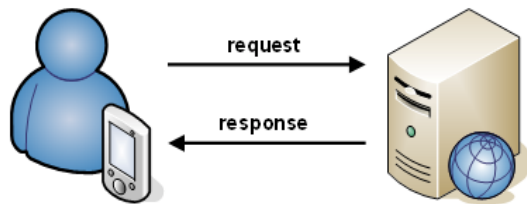


[Eckert2001]

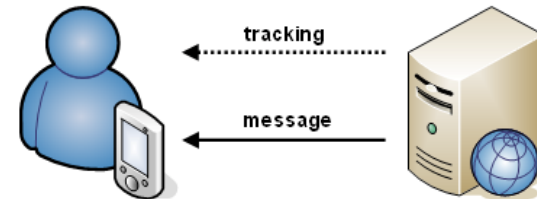
Location-based Services

- Unter 'Location Based Services' (LBS) sind standortbezogene Dienste zu verstehen. Diese stellen selektive Informationen mittels Zeit- und Positionsabhängiger Daten für den Nutzer zur Verfügung.
- Kategorisierung:

Reaktive Dienste



Proaktive Dienste



[Schiller und Voisard, 2004]
[Küpper, 2005]



Allgemeine Zugriffskontrollstrategien

- Jeder Zugriffsversuch soll kontrolliert werden und diese Kontrolle darf nicht umgangen werden.

[Eckert2001]

- Bekannte Zugriffskontrollstrategien
 - DAC (Discretionary Access Control)
 - MAC (Mandatory Access Control)
 - RBAC (Role Based Access Control)

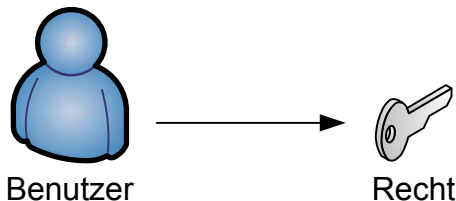


DAC (Discretionary Access Control)

- Benutzerbestimmbare Zugriffskontrollstrategie
- Jedem Objekt ist ein Subjekt als Besitzer zugeordnet. Dieser ist verantwortlich für Zugriffsrechtevergabe..

Zugriffskontrolllisten

subjekt_name, zugriffsrechte



```
Alice, rwx  
Bob, rx  
Carl, r  
Dan, rwx  
...
```

Nachteil: Schlechte Skalierbarkeit

→ In Umgebungen mit vielen Benutzern und verschiedenen Rechten problematisch
(bei langen Listen aufwendiges, ineffizientes durchsuchen)

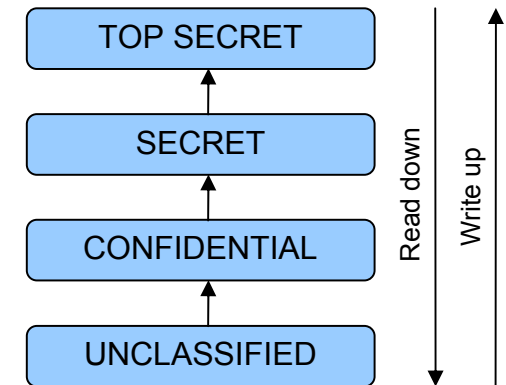


MAC (Mandatory Access Control)

- Systembestimmte Zugriffskontrollstrategie
- Zugriffsschutz über Vertraulichkeitsstufen (Jeder Benutzer erhält eine Freigabe für eine der Vertraulichkeitsstufen)
- (Basis = {Vertraulichkeitsstufen})

Regeln:

- Read-Down-Regel
 $\text{Vertraulichkeitsstufe}[\text{Objekt}] \leq \text{Vertraulichkeitsstufe}[\text{Subjekt}]$
- Write-Up-Regel
 $\text{Vertraulichkeitsstufe}[\text{Objekt}] \geq \text{Vertraulichkeitsstufe}[\text{Subjekt}]$



Nachteil:

Vertraulichkeitsstufen sind statisch

→ In Umgebungen mit häufig wechselnden Anforderungen zu unflexibel



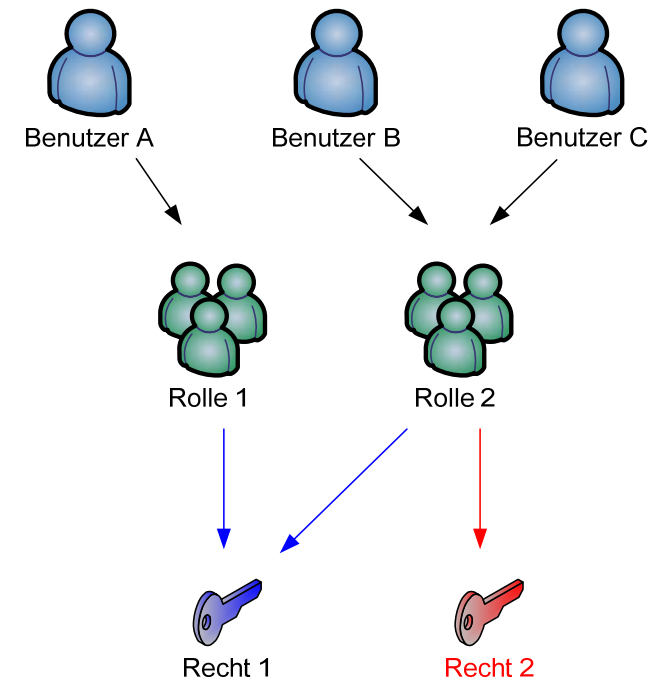
RBAC (Role Based Access Control)

- Rollenbasierte Zugriffskontrollstrategie
- Einem Subjekt werden (seinen Aufgaben entsprechend) Rollen zugewiesen
- Entkopplung der Benutzer von Rechten
- Rollenhierarchien sind möglich (geringerer Wartungsaufwand)
- 'Principle of Least Privilege'
nur so viele Rechte wie nötig

Vorteil:

Bessere Skalierbarkeit

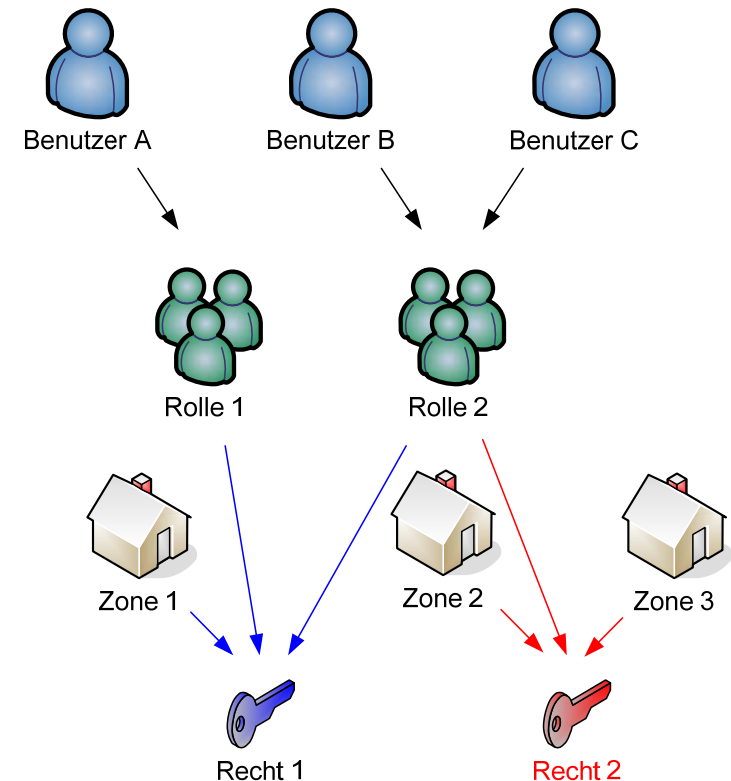
→ Sehr gut geeignet für Systeme mit einer großen Anzahl von Nutzern





Zugriffskontrollstrategie für LBS

- SRBAC (Spatial Role Based Access Control)
Ortsabhängige, rollenbasierte Zugriffskontrollstrategie
- Zugriffsberechtigung zusätzlich zur Rolle noch vom Sicherheitskontext (Ort) abhängig
- Ort des Requests muss bekannt sein
Verschiedene Orte müssen definiert werden



Vorteil:
Bessere Skalierbarkeit

→ Sehr gut geeignet für Systeme mit einer großen Anzahl von Nutzern

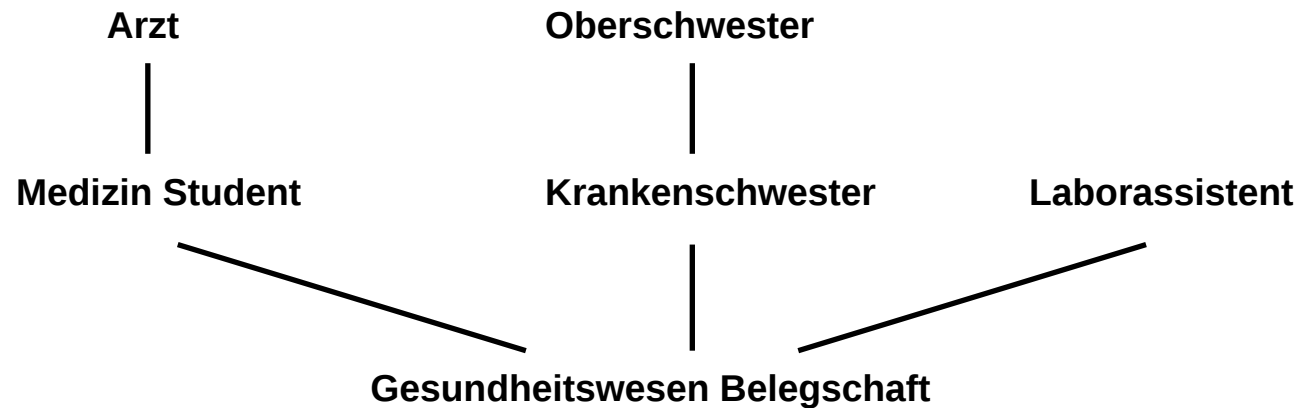


Zugriffskontrollstrategie für LBS

Beispiel: Ortsbezogene Rechtetabelle

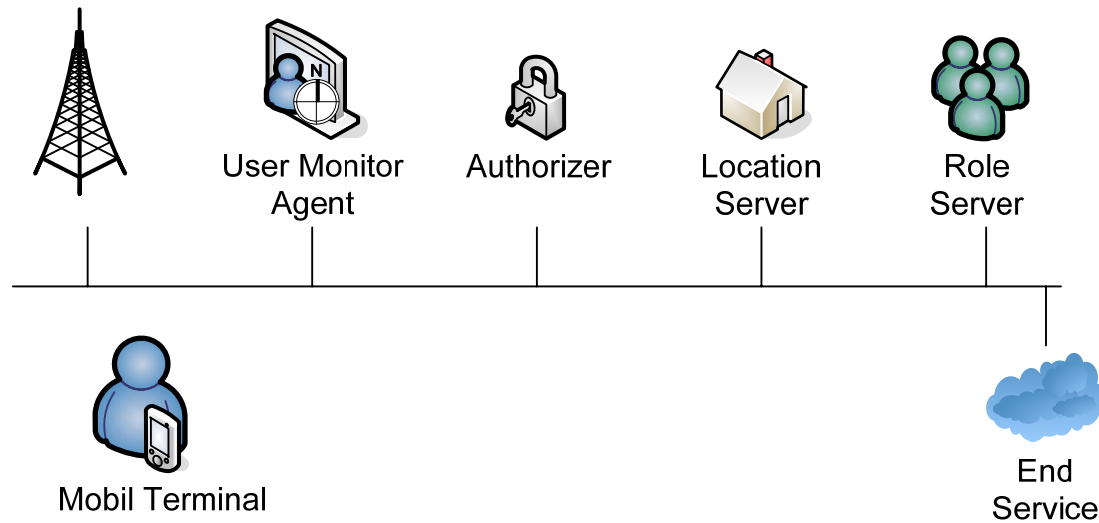
Rollen	Orte	Rechte
<i>Rolle1</i>	<i>Zone1</i>	<i>Recht1, Recht2, Recht3</i>
<i>Rolle1</i>	<i>Zone2</i>	<i>Recht4</i>
<i>Rolle1</i>	<i>Zone3</i>	∅

Beispiel: Rollenhierarchie





Framework für mobile Geräte

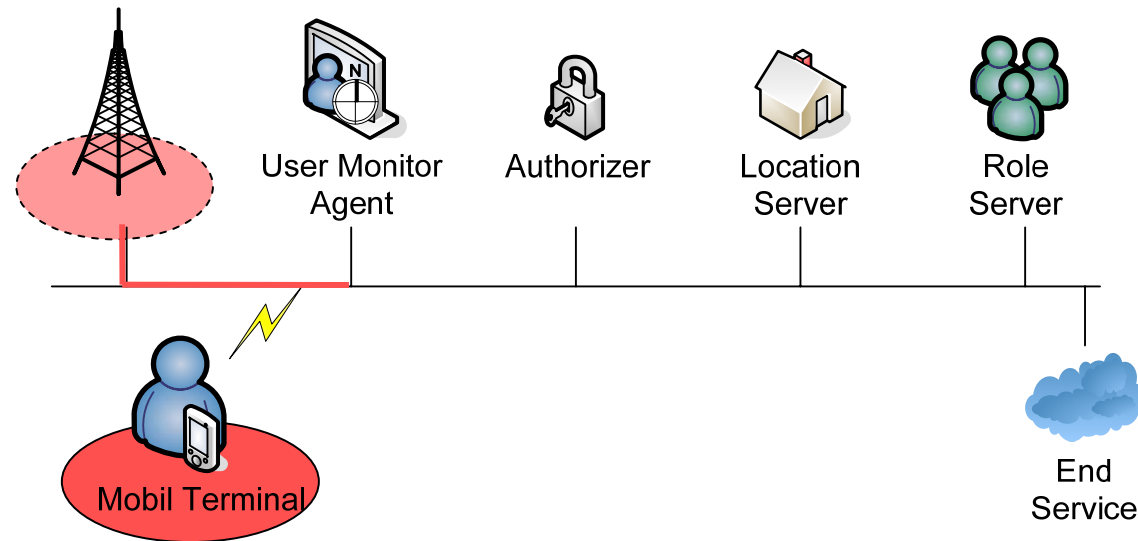


Framework für sicheren Zugriff auf Daten von mobilen Geräten



Framework für mobile Geräte

Mobile Termial

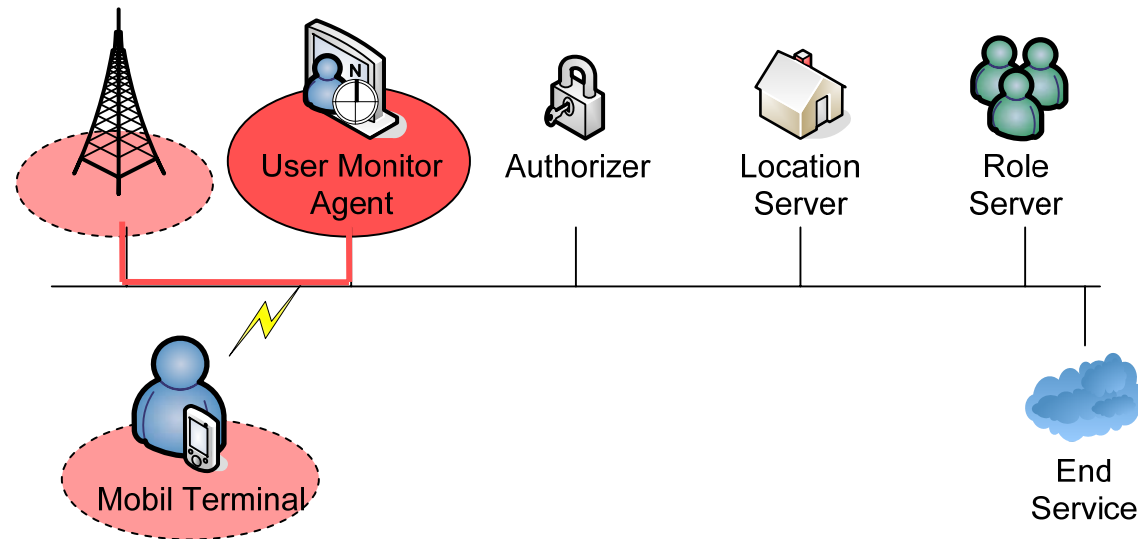


- Repräsentiert Benutzer des mobilen Gerätes
- Ausführungsumgebung kontrolliert laufende Dienste



Framework für mobile Geräte

User Monitor Agent

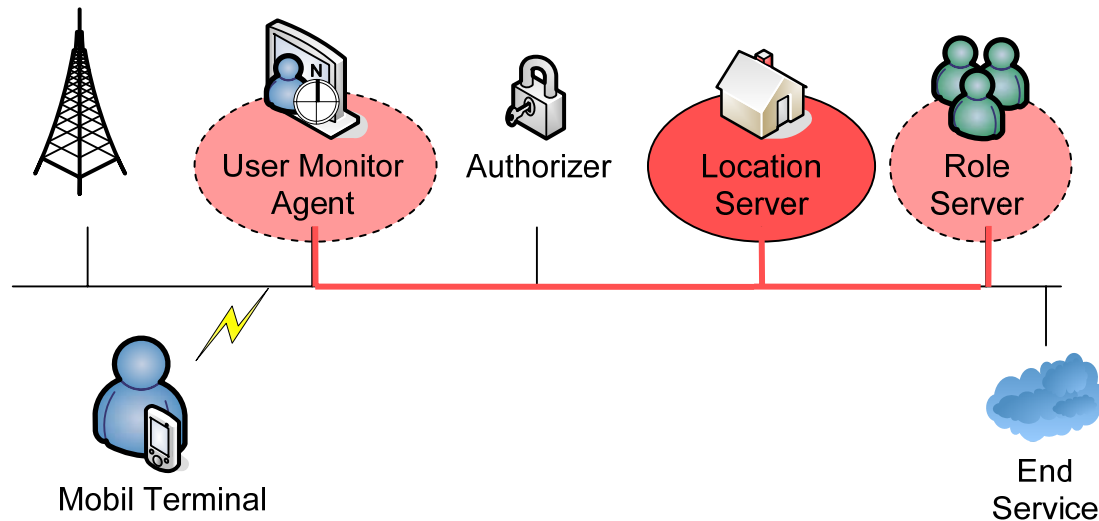


- Erfasst Position von aktiven Benutzern
- Daten werden von Locationssensoren der Geräte eingesammelt



Framework für mobile Geräte

Location Server

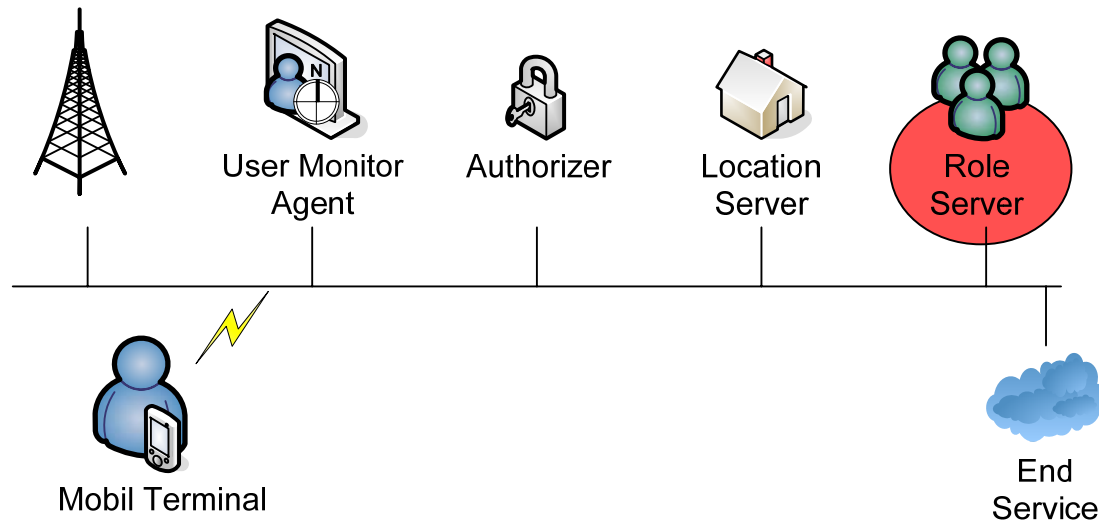


- Sammelt physikalische Positionsdaten von aktiven Benutzern vom *'User Monitor Agent'*
- Informationen werden anschließend bei Änderung des Ortes an den *'Role Server'* weitergegeben (location update message)



Framework für mobile Geräte

Role Server

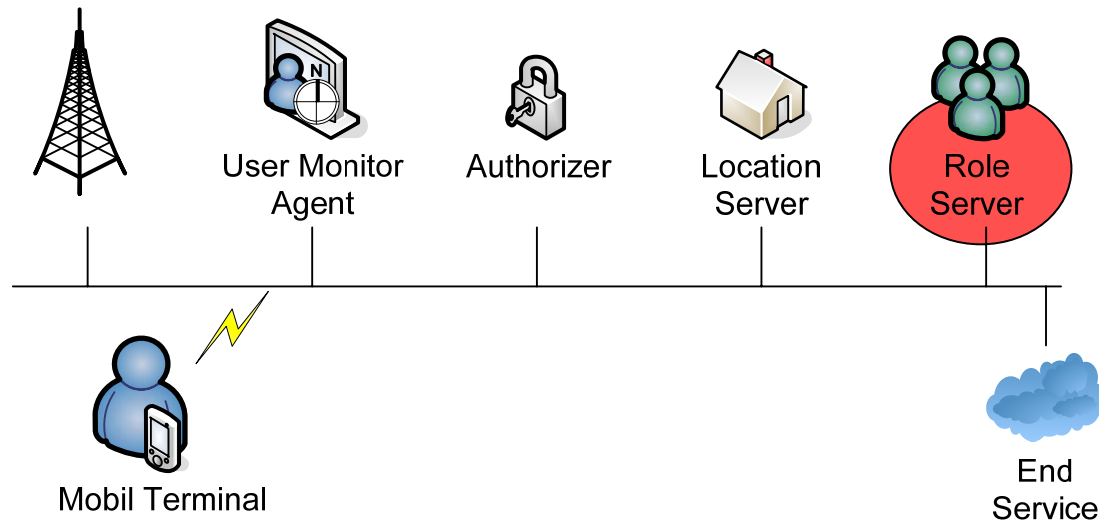


- Beinhaltet Tabelle mit der Zuordnung der
 - Benutzer zu Rollen
 - Rechte zu Rollen
 - Einschränkungen der SRBAC-Komponente



Framework für mobile Geräte

Authorizer

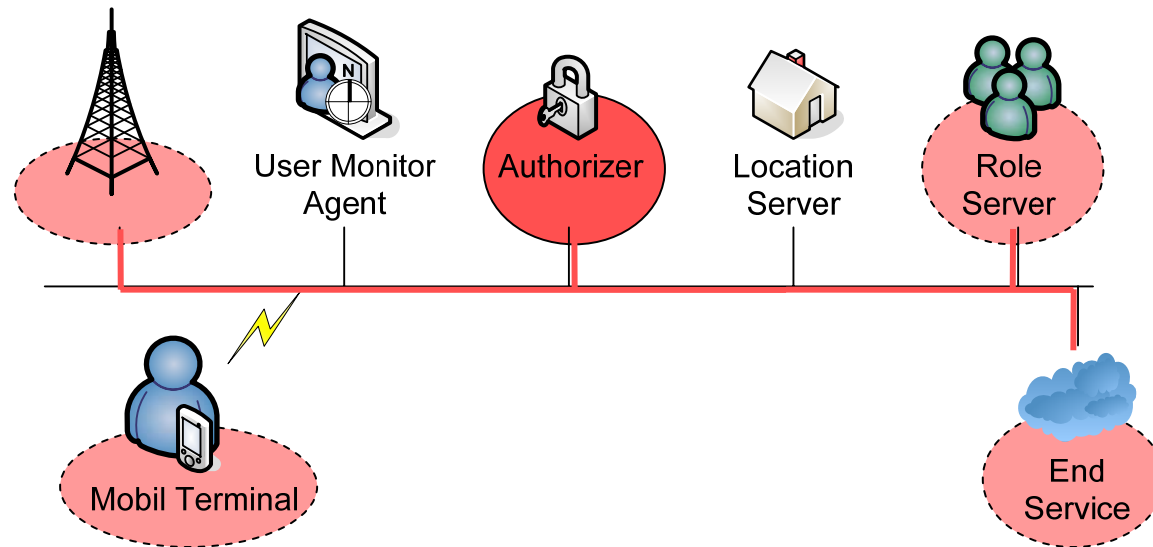


- Statusinformationen aktiver Rollen
- Empfängt die logischen Ortsinformationen vom `Location Server`
- Sendet einen aktuellen Rechtesatz an Authorizer



Framework für mobile Geräte

Authorizer



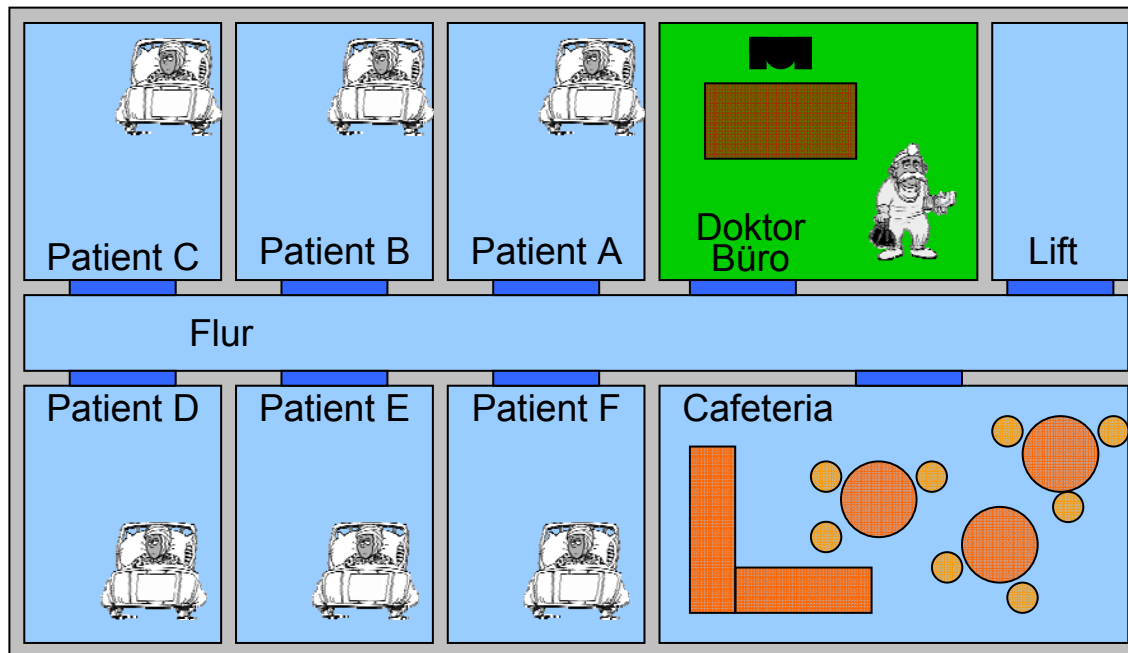
- Kümmt sich um Anfrage vom `Mobil Terminal`
- Fordert aktuellen Rechtesatz vom `Role Server` an
- Rechtesatz wird im Entscheidungsprozess verwendet

Szenario

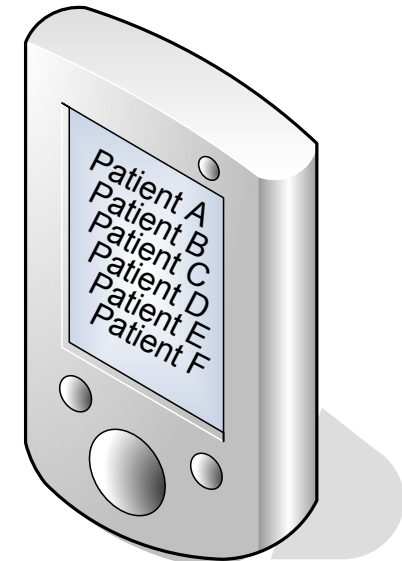


Doktor auf Visite

Szenario

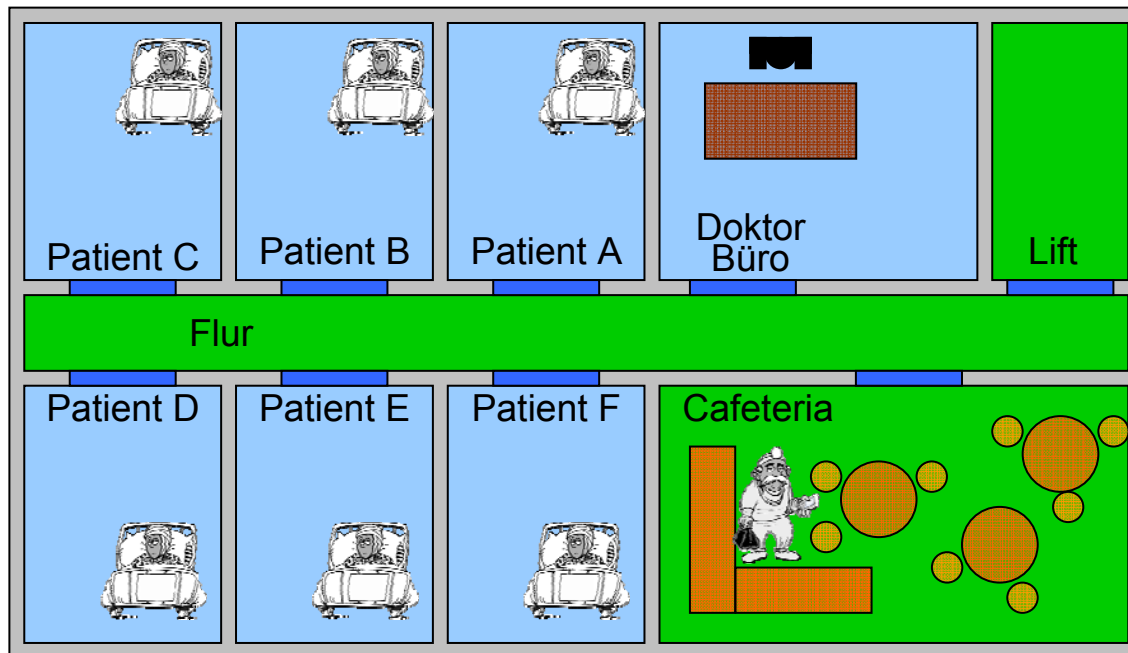


Doktor Büro

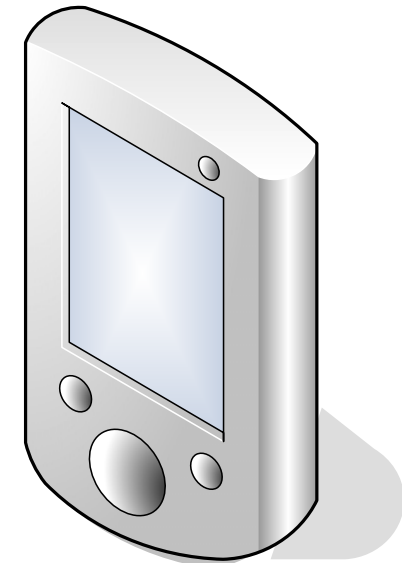


Zugriff auf alle Patientendaten
- Daten lesen u. schreiben -

Szenario

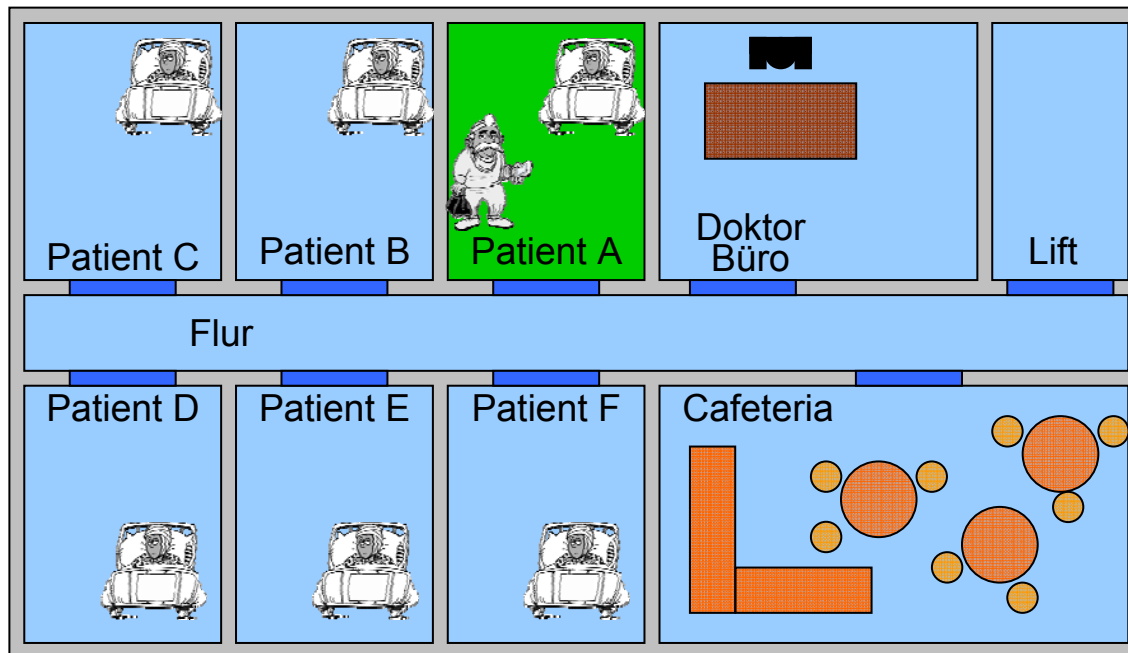


Flur / Cafeteria / Lift



Keine Patientendaten sichtbar

Szenario



Raum Patient A



Teile der Patientendaten
von Patient A
- Daten lesen u. schreiben -



Zusammenfassung

- Entstehen durch Kenntnis des Ortes neue Sicherheitsanforderungen?

Nein. Bekannte Sicherungstechniken für Drahtlose Netzwerke können verwendet werden. (Eike)

aber

Im Bereich Privacy schon..

- Kann die Sicherheit durch Kenntnis des Ortes verbessert werden?

Ja.

- Feingranularer (bestimmte Aktionen nur von bestimmten Orten)
 - nicht nur Identität / Gerät stehlen
 - Unschuldsnachweis wird erleichtert
- Im Beispiel Krankenhaus können Fehler vermieden werden (nicht versehentlich den falschen Patienten operieren..)

- Projekt im 3. Semester
 - `Mobiles mehrbenutzerfähiges tolles Spiel`
 - Vorläufiger Projektname: `*Pervasive-Gaming Framework*`
 - Spielidee: Schnitzeljagd
- Kompromiss aus verschiedenen Themenschwerpunkten
(unter anderem Location Based Services)

- [Eckert 2001] ECKERT, Claudia: IT-Sicherheit Konzepte-Verfahren-Protokolle. Oldenbourg Verlag München Wien, 2001
- [Küpper 2005] KÜPPER, Axel: Location-Based Services Fundamentals and Operation. John WILEY & Sons, Ltd., 2005
- [Hansen und Oleshchuk 2003] HANSEN, Frode ; OLESHCHUK, Vladimir: Spatial Role-Based Access Control Model for Wireless Networks. In: IEEE (2003).
- [Hansen und Oleshchuk 2006] HANSEN, Frode ; OLESHCHUK, Vladimir: Location-based Security Framework for use of Handheld Devices in Medical Informaiton Systems. In: IEEE (2006).
- [Ferraiolo u. a. Apr. 2003] FERRAIOLO, David F. ; KUHN, D R. ; CHANDRAMOULI, Ramaswamy: Role-Based Access Controls. Artech House, Apr. 2003
- [Schiller und Voisard 2004] SCHILLER, Jochen ; VOISARD, Agnès: Location-Based Services. Elsevier Inc. - Morgan Kaufmann Publishers, 2004
- [Zhang u. a. June 2002] ZHANG, Longhua ; AHN, Gail-Joon ; CHU, Bei-Tseng: A Role-Based Delegation Framework for Healthcare Information Systems. In: ACM (June 2002)
- ...



Ende

Vielen Dank!

Fragen?