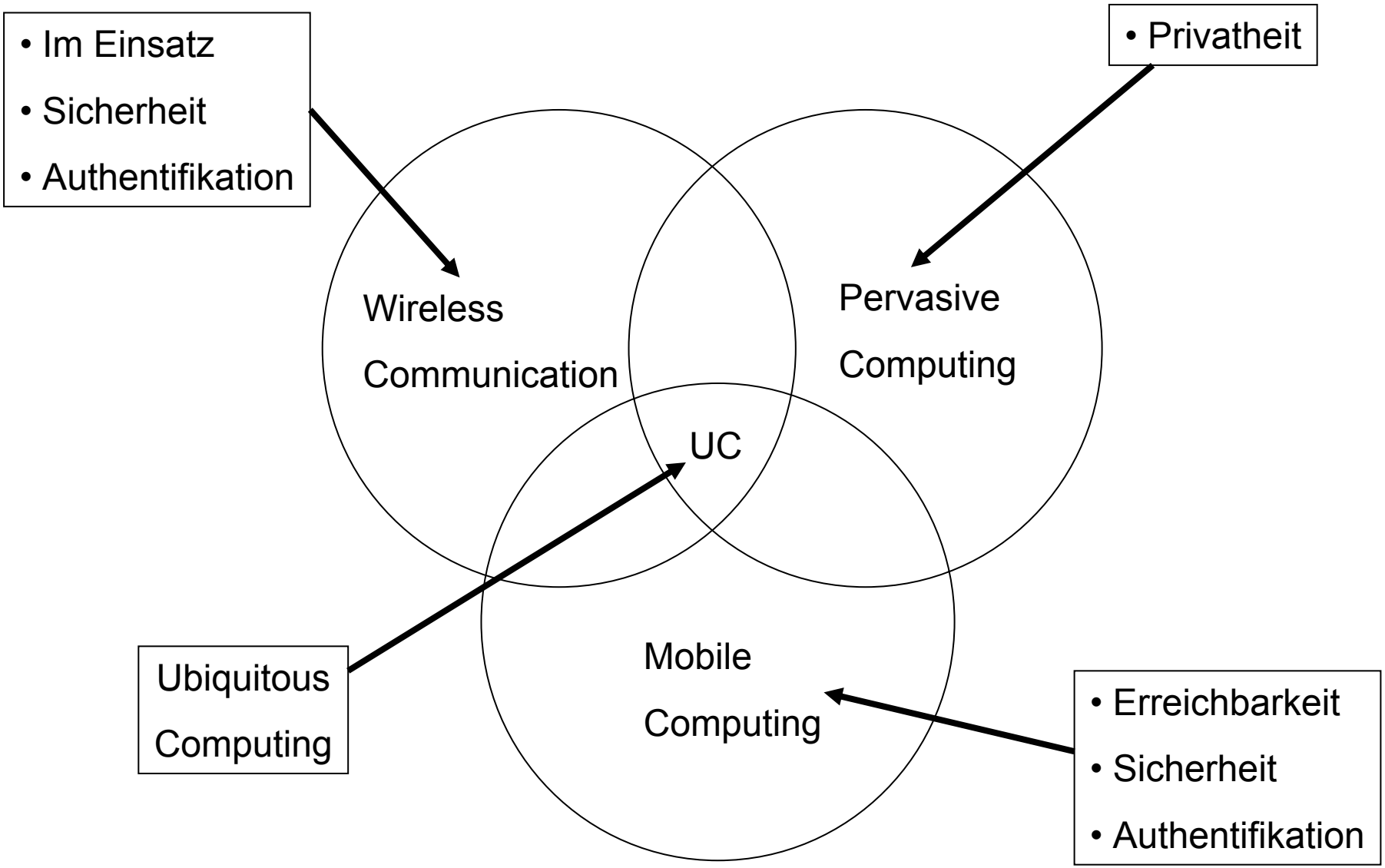
Ad-hoc-Authentifikation und *Kontext* in EMIKA

a) **Einführung in das Projekt EMIKA (Prof. Dr. Müller)**

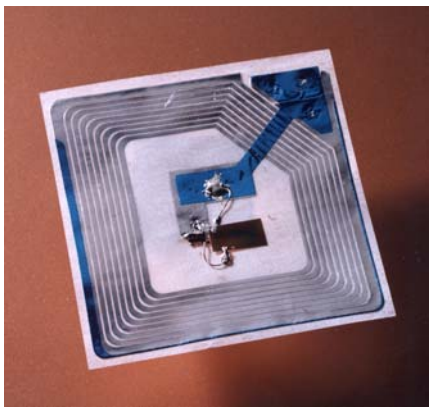
b) **Ad-hoc-Authentifikation (Kähmer, Kreutzer)**

Workshop „Kontext“

TU Stuttgart, 23. 7. 2003

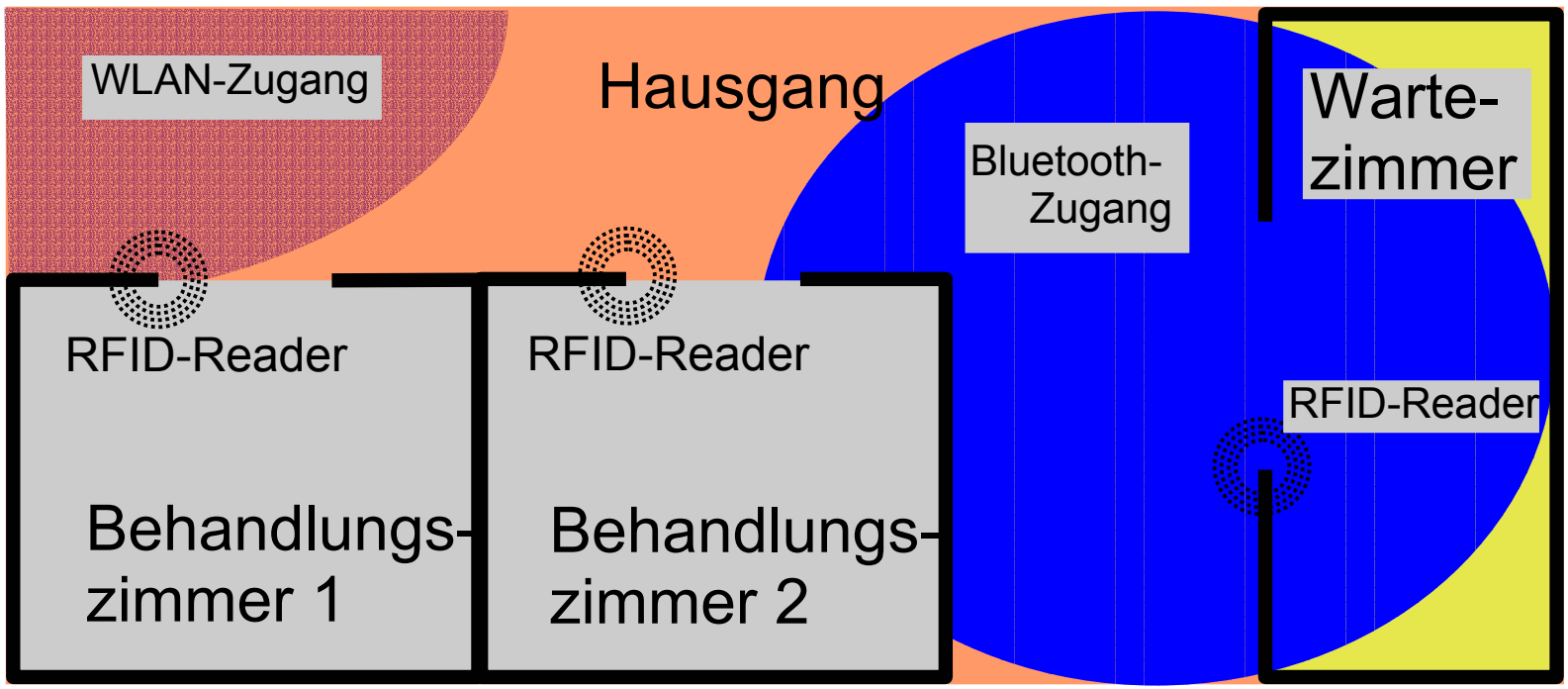

• Im Einsatz
• Sicherheit
• Authentifikation
• Privatheit
Wireless Communication
Pervasive Computing
UC
Mobile Computing
Ubiquitous Computing
• Erreichbarkeit
• Sicherheit
• Authentifikation

Szene aus der Patientenlogistik in der Radiologie (Projekt EMIKA)

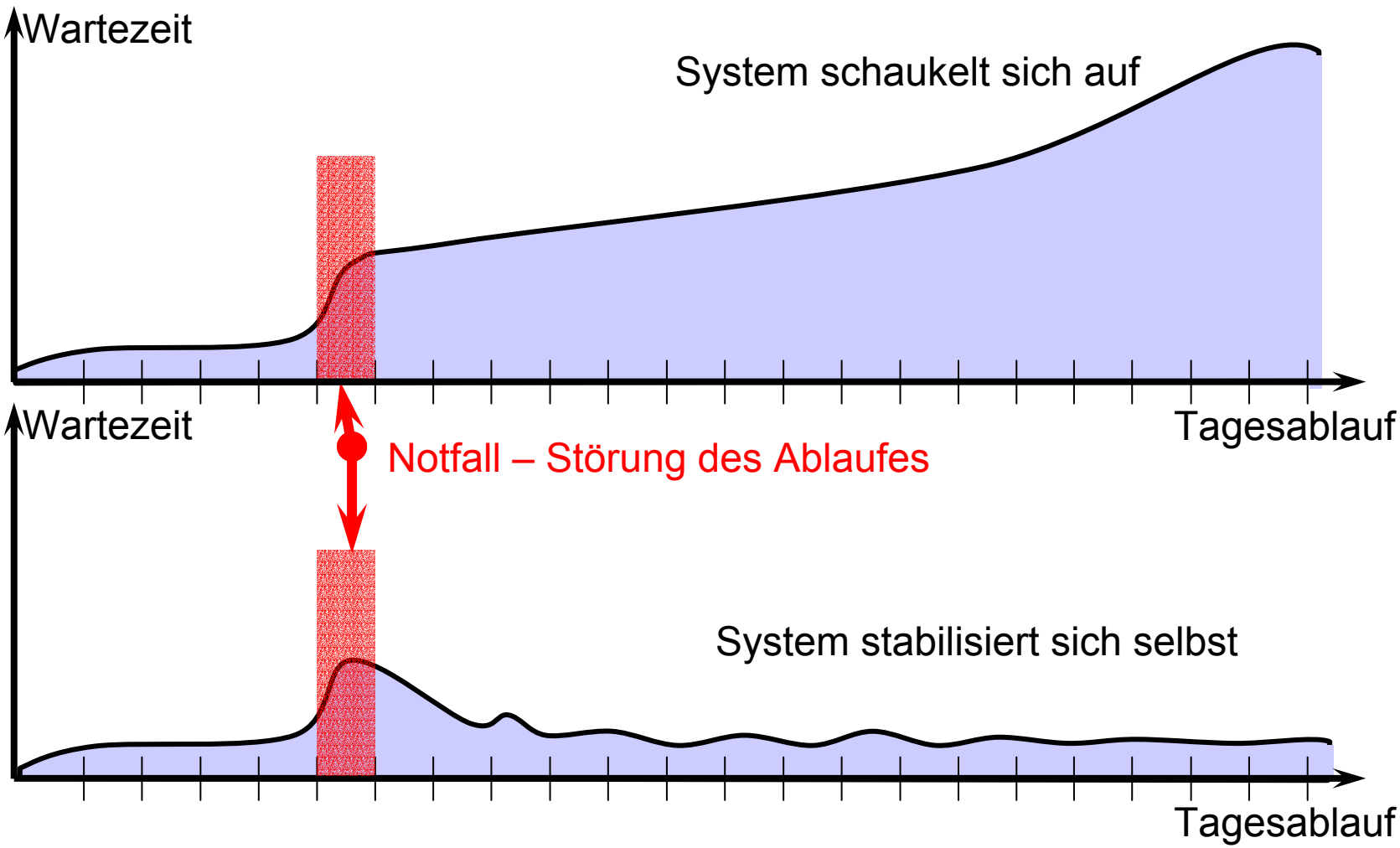


Terminplanung und Logistik in EMIKA-Radiologie:

- Personal (Identität, Abteilung, Qualifikation, aktueller Aufenthaltsort …)
- Patienten (Identität, Diagnose, aktueller Aufenthaltsort, …)
- Räume (Gebäude, Stockwerk, Raumnummer, Funktion, …)
- Geräte (Diagnostik, Bildformate, Dauer, Verfügbarkeit, …)



Experiment EMIKA: im Modell



Ad-hoc-Authentifikation und *Kontext* in EMIKA

Projektgruppe: Martin Kähmer, Michael Kreutzer, Sumith Chandratilleke

Grund für Ad-hoc-Authentifikation

Im EMIKA-Projekt:

- große Anzahl an Geräten, die sich via Funk spontan miteinander vernetzen können
- daher: Vielzahl von potentiellen Kommunikationsbeziehungen

Es soll nicht jedes Gerät mit jedem anderen reden:

- Skalierungsproblem
- Verwechselungsgefahr
- Sicherheit: man-in-the-middle
- …

Authentifikation vs. Ad-hoc-Authentifikation

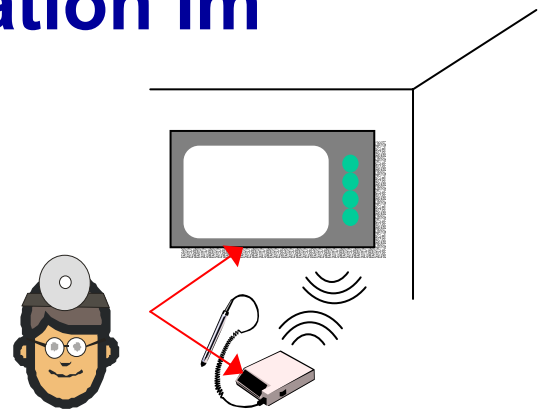
Authentifikation

- gemeinsames Geheimnis wie Benutzername/Passwort
- Überprüfung der Identität

Ad-hoc-Authentifikation

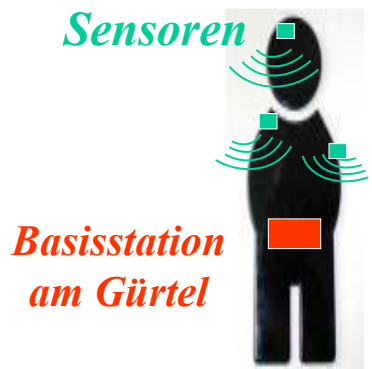
- Vorab ist keine gemeinsame Wissensbasis vorhanden.
- Gemeinsames Wissen wird spontan durch Präauthentifikation erstellt
- Anschließend kann Authentifikation durchgeführt werden.

Beispiele für Ad-hoc-Authentifikation im EMIKA-Projekt



– Arzt “verknüpft” ein Diagnosegerät mit einem Display an der Wand für weitere Befundung

– Personal Health Monitoring [http://www.phmon.de/]
Messung von Vitalparametern wie:
  - ***Atmung***
  - ***Blutdruck/Sauerstoff***
  - ***EKG (Herz)***
  - ***IOP (Augeninnendruck)***



Probleme Ad-hoc-Authentifikation

Heutige Authentifikationsprotokolle (wie SSL, Kerberos)

- gehen von gemeinsamen Vorwissen aus (Geheimnis, Zertifikate)
- basieren auf Public-Key-Kryptography (hoher Ressourcenverbrauch)

Verwandte Arbeiten

Balfanz et al. lösen das Problem des gemeinsamen Vorwissens in Ad-Hoc-Netzen mit einem 2-Phasen-Verfahren [BSSW02]

1. Präauthentifikation: Austausch der Public-Keys auf einem *sicheren* Kanal mittels IrDA
2. Authentifikation mit Hilfe der Public-Keys

[BSSW02] D. Balfanz, D. Smetters, P. Stewart and H. Wong: Talking to strangers: Authentication in adhoc wireless networks In Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California

Zusätzliche Anforderungen an Authentifikation durch EMIKA

- Einbindung ressourcenschwacher Geräte
  (insbesondere unterstützen nicht alle Geräte Public-Key-Verfahren!)
- Je nach Anwendung geeignetes Verfahren zur Herstellung eines gemeinsamen Geheimnisses

Unser Ansatz:

1. **Präauthentifikation mittels Kontext**
   Ziel: Sichere Methode zur Erzeugung eines gemeinsamen Vorwissens durch die Erkennung eines *gemeinsamen Kontextes*.
2. **Eigentliche Authentifikation**
   Mit Standardverfahren oder leichtgewichtiger, wie in [CK03] beschrieben

[CK03] Sumith Chandratilleke, Michael Kreutzer: Credential-basierte Ad-hoc-Authentifikation, netzwoche Netzguide E-Security 2003 (März 2003), ISBN 3-907096-04-5

Präauthentifikation mittels Kontext

Gemeinsamer Kontext zum Bekanntmachen von Geräten

Passive Nutzung von Kontext:

- bestehender Kontext zur individuellen Situationsbestimmung

Aktive Nutzung von Kontext:

- willentlich hergestellter gemeinsamer Kontext

Angedachte Verfahren für Präauthentifikation mittels Kontext

- Zeichenfolge eingeben (PIN)
- Elektrischer Kontakt (z.B. “Fill Gun”)
- Infrarot-Kommunikation

- Gemeinsames akustisches Ereignis
- Gemeinsames optisches Ereignis
- Smart-Its Friends (Schütteln) [http://www.smart-its.org/]
- Gleichzeitige oder zeitlich nahe Erfassung biometrischer Merkmale

Forschungsfrage

- Ist Kontext ein Konzept, um im EMIKA-Projekt die Authentifikation zwischen Geräten zu vereinfachen?

Zur Diskussion:

- Ist bisheriger Kontext-Begriff „zu eng“
- Realisierung der zeitlichen und räumlichen Beschränkung der Präauthentifikation
- Nutzerschnittstelle: Realisierung des willentlichen Aktes
- …