

Sicherheit von Wearables

Akademietag
18/19 April 2008

Zied Ghrairi
Hochschule Bremen

Agenda

- Wearable Computing
- SiWear-Projekt
- Sicherheit
- Fazit

Was ist Wearable Computing?

Wearable Computer

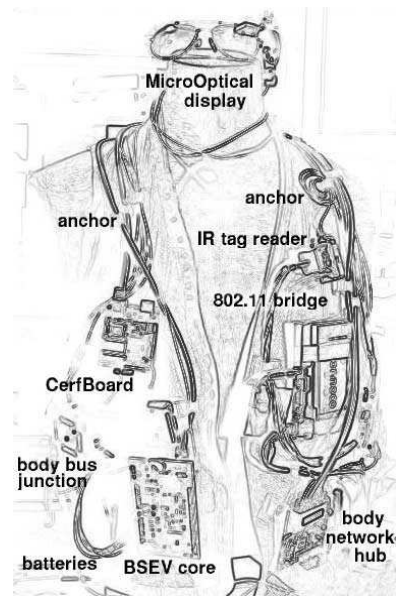
- tragbarer Computer
 - Befestigung am Körper des Benutzers



Quelle: ETH Zürich

Wearable Computer

- Miniaturisierung der Komponenten
- Komponenten in der Kleidung integriert



Quelle: ETH Zürich

Wearable Computer

- Problem: Benutzerakzeptanz
 - Benutzbarkeit
 - unzureichender Prozessintegration
 - Sicherheitsbedenken



Sichere Wearable-Systeme zur Kommissionierung industrieller Güter sowie für Diagnose, Wartung und Reparatur

- Gefördert durch das BMWi im Förderschwerpunkt SimoBIT
- Laufzeit: 30 Monate
- Start: September 2007
- www.siwear.de

Partner

- SAP
- Daimler AG
- NeoBusiness Partners GmbH
- teXXmo Mobile Solution GmbH & Co. KG
- MRC, HSB, TZI, BIBA

Projektziel

- Erarbeitung eines Konzepts für eine Sicherheitsarchitektur
 - Keine Neuentwicklung von Sicherheitsmechanismen
 - Standardisierung des Konzepts
- **sichere** Kommunikation
- **sichere** Authentisierung
- **sichere** Lokalisierung
- **benutzbare** Benutzungsschnittstellen

Sicherheitsziele

- Vertraulichkeit / Confidentiality
- Integrität / Integrity
- Verfügbarkeit / Availability
- Authentizität / Authenticity
- Datenschutz / Privacy

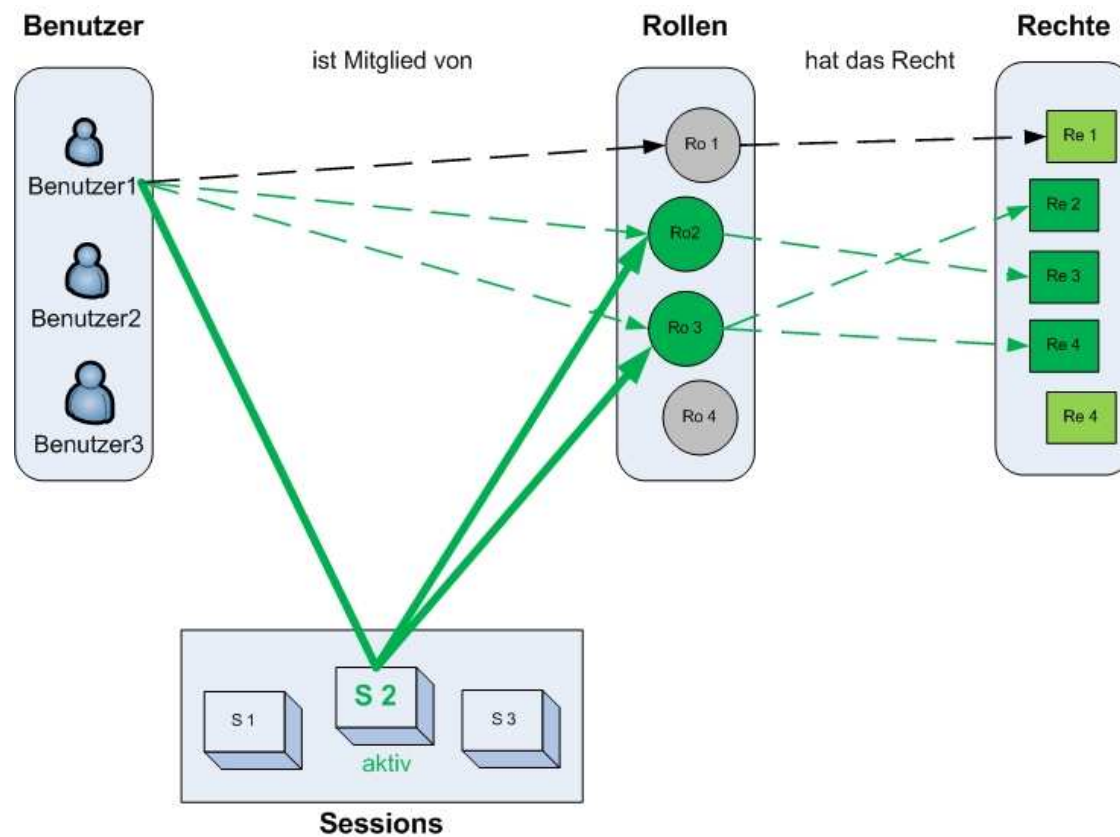
Vertraulichkeit

- Schutz der auf Endgeräte gespeicherten Daten
- Schutz der übertragenen Daten
 - Drahtlose Kommunikation: Wer hört mit?
 - Schutz gegen aktiven und passiven Angriffen

Vertraulichkeit

- TrueCrypt, SecureDoc,
- WPA (TKIP), WPA2(CCMP)
- VPN
 - IPSEC, SSL, PPTP, L2TP
- Zugriffskontrolle (Rechtvergabe)
 - ACL, CL, RBAC

RBAC (engl. Role-Based Access Control)



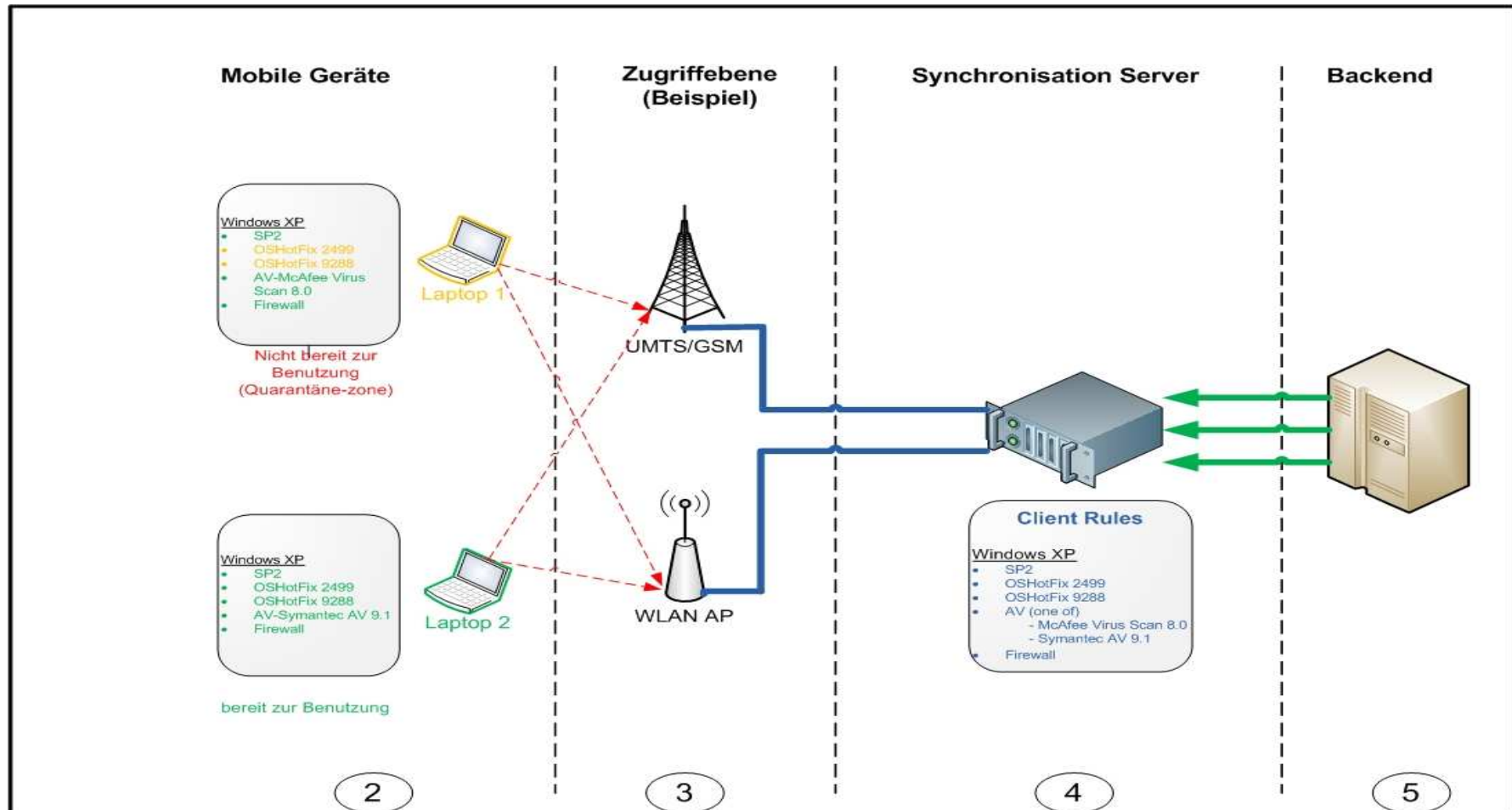
Integrität

- Wer schreibt?
- Schutz vor unautorisierter sowie unbemerkter Veränderung der Daten. Wie?
 - Zugriffskontrolle
 - Hashwerte
 - Digitale Signature

TNC: Trusted Network Connect

- Mechanismus zur Zugangskontrolle
 - von Trusted Computing Group entwickelt
 - Kontrolle der im Gerät vorhandenen Software und Hardware
 - Prüfung der Sicherheitsrichtlinien
- Nur vertrauenswürdige eingestufte Wearable Computer zur Kommunikation in einem Netzwerk zugelassen

Integrität



Verfügbarkeit

- das ständig geforderte Sicherheitsziel
- Verfügbarkeit von:
 - IT-Systemen
 - Informationen

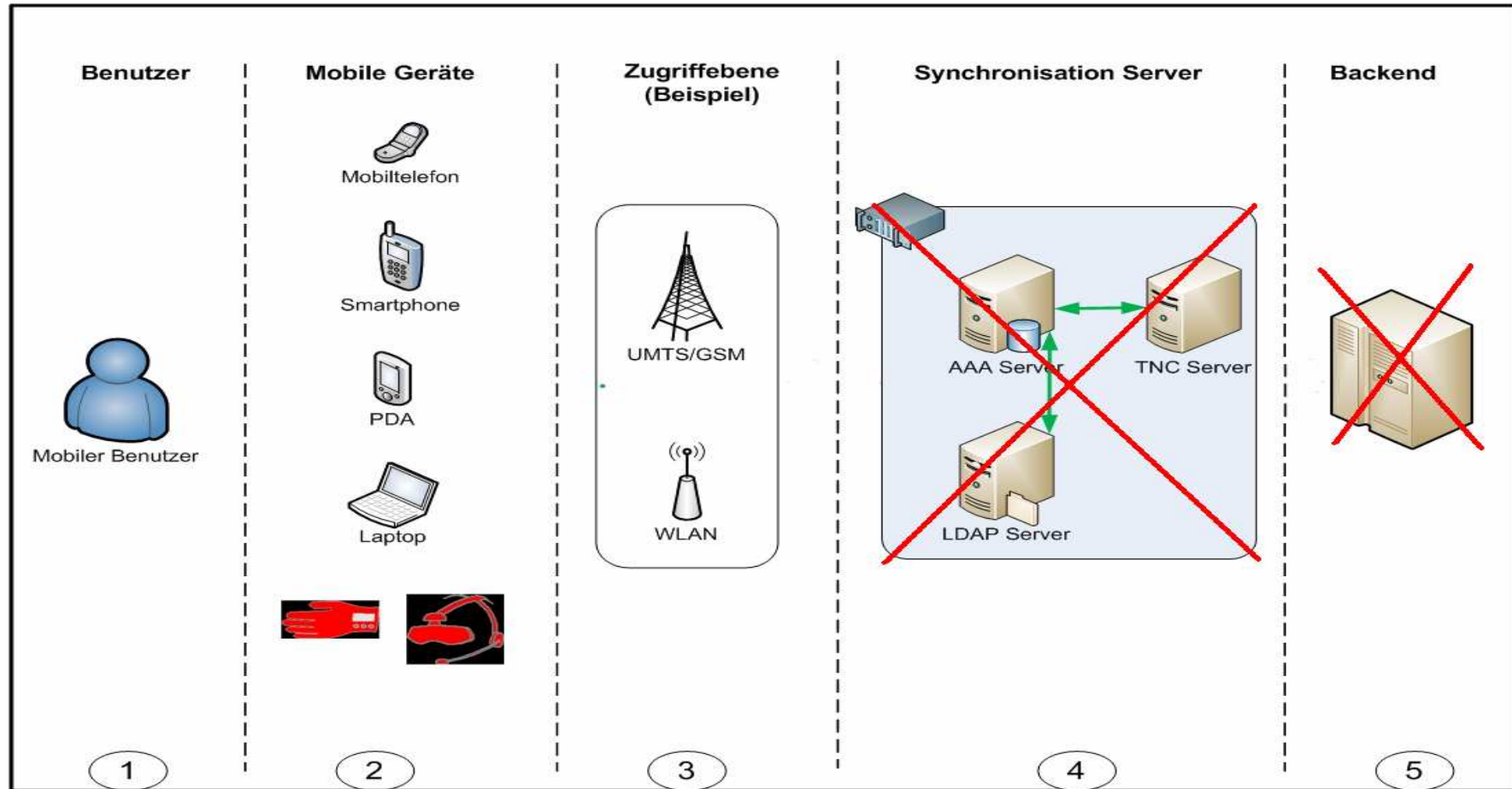
Verfügbarkeit

- Verlust:
 - Lokalisierung der mobilen Geräten
- Device Management:
 - Installation, Konfiguration, Fehlerbeseitigung
 - zentrale Datensicherung und -wiederherstellung
 - Zerstörung der Daten auf Wearables bei Diebstahl oder Verlust
 - Sperrung der Endgeräte

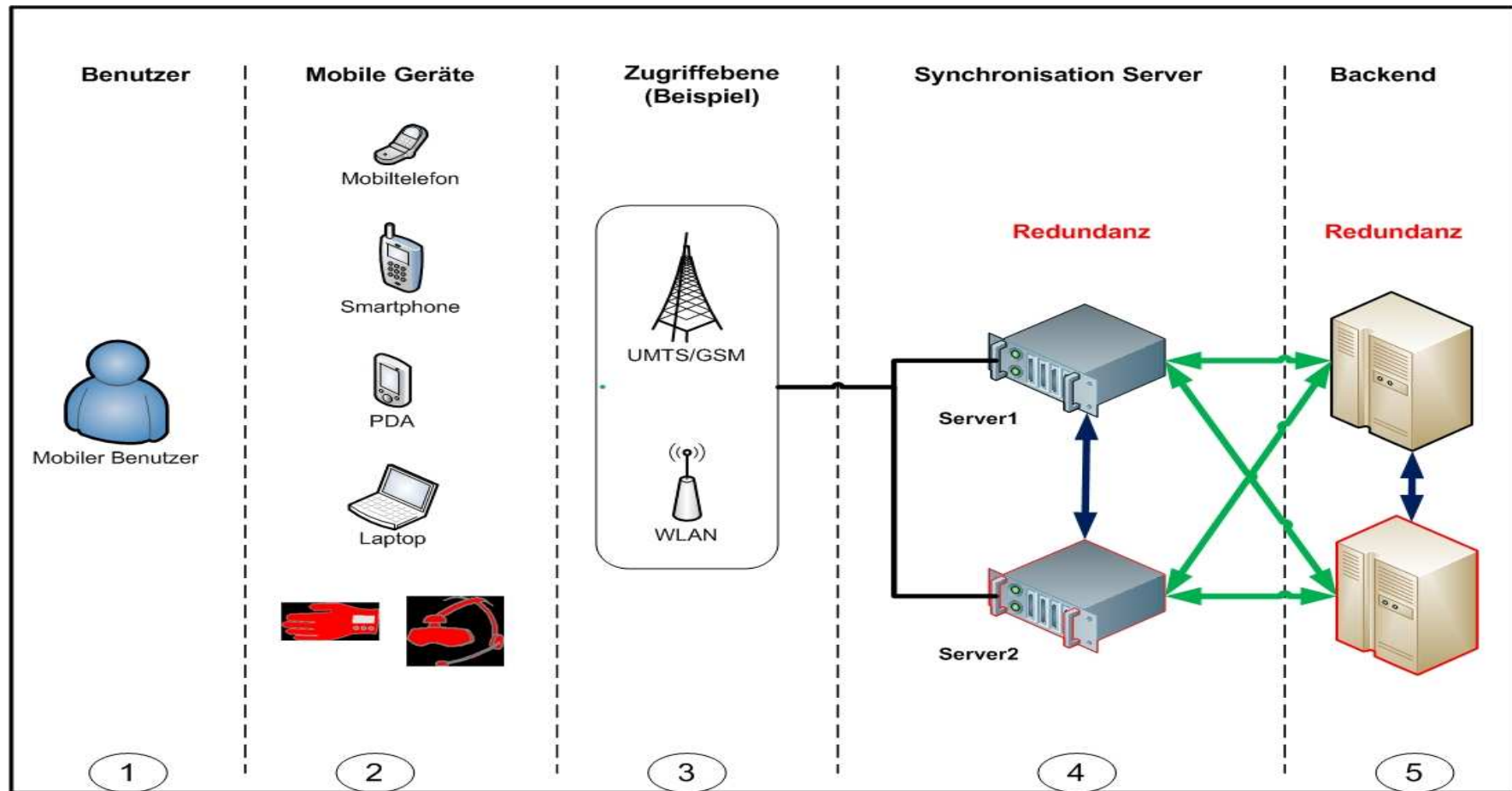
Verfügbarkeit

- Batterielaufzeit: Das größte Problem bei Wearable Computern
- Wearables müssen stets mit Strom versorgt werden
- Ziel: Optimierung des Energieverbrauches
 - Kontextsensitivität und intelligentes Standby Management
 - Benutzer selber als Energieversorger

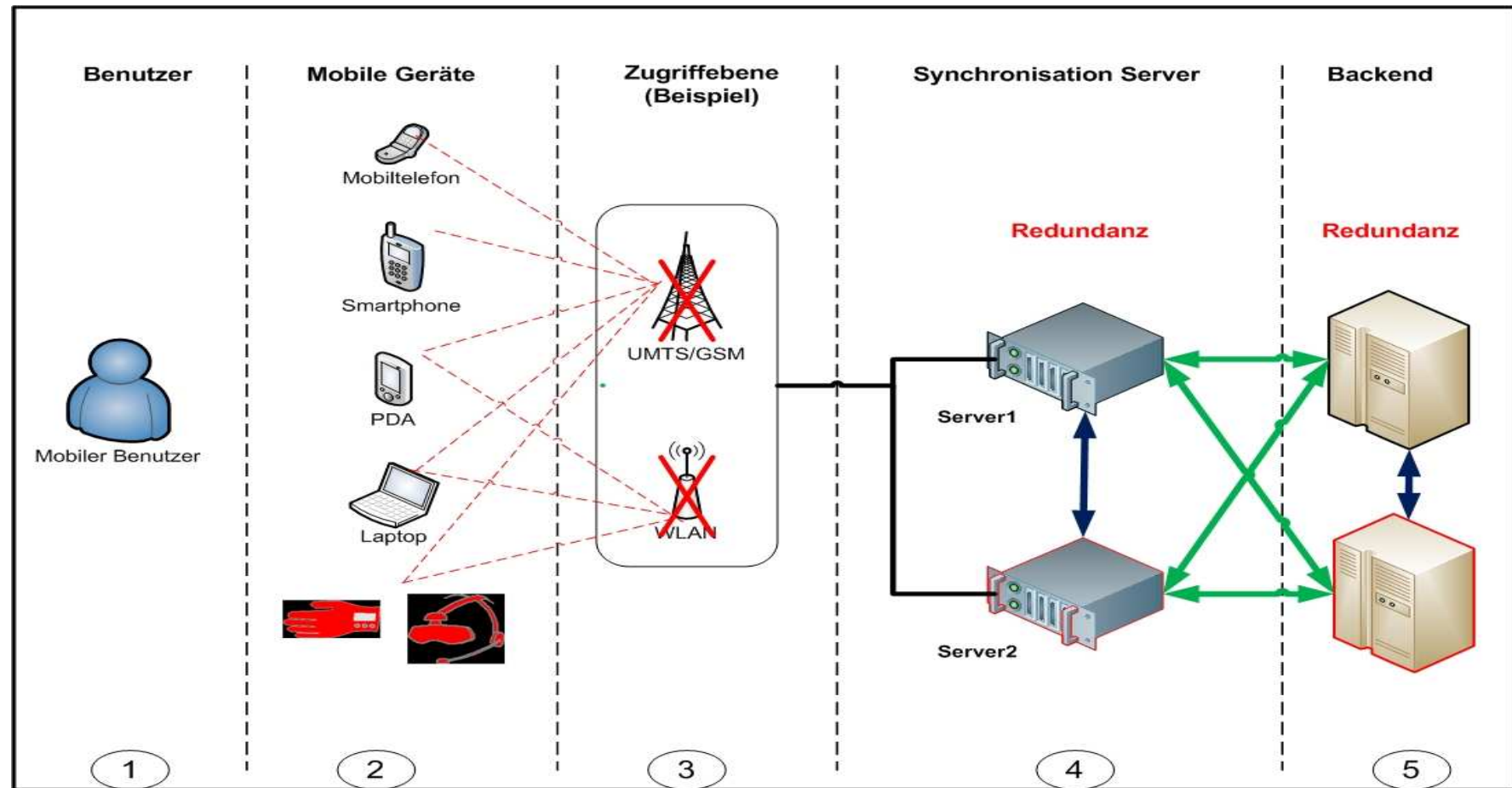
Verfügbarkeit



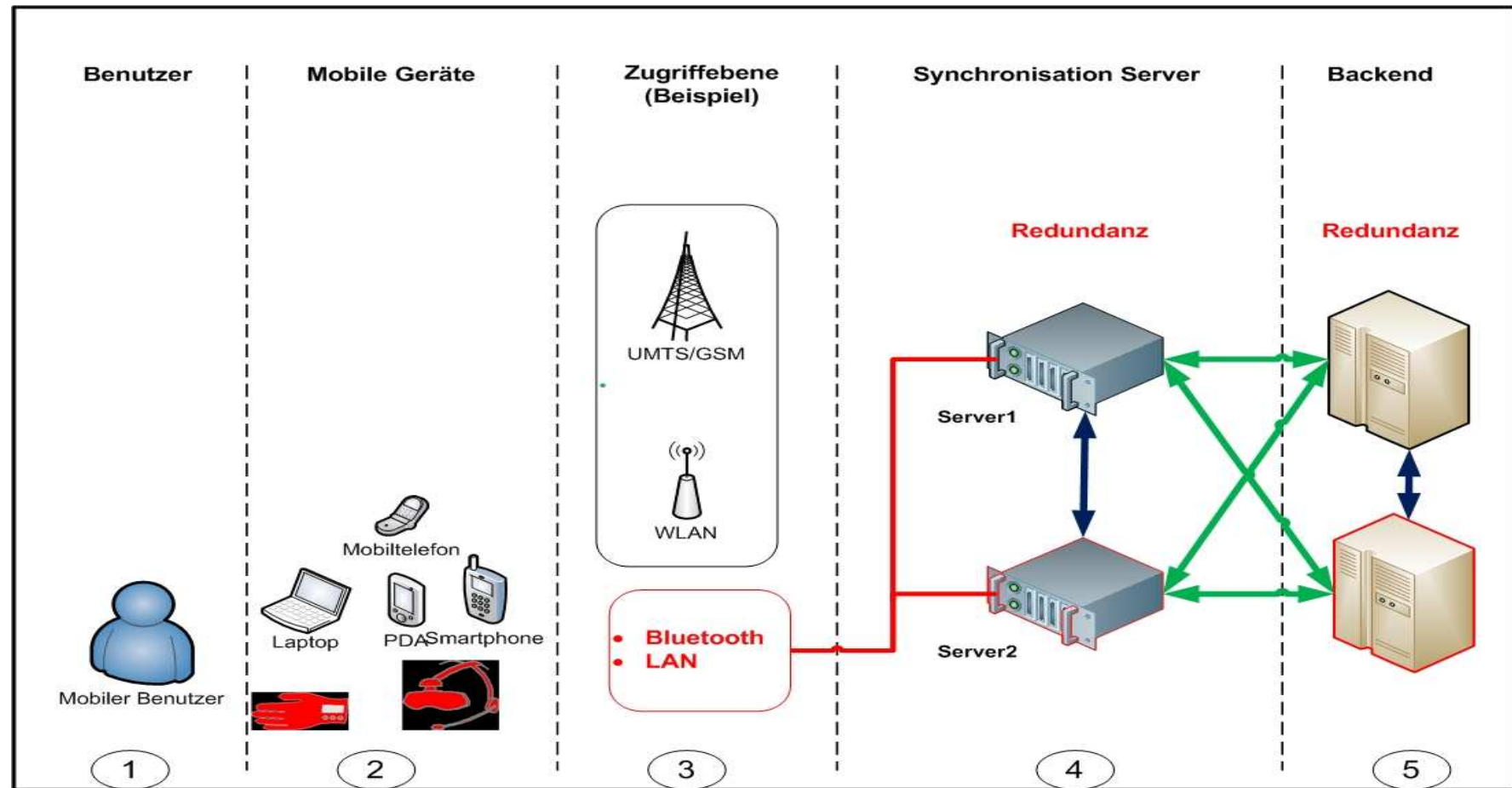
Verfügbarkeit



Verfügbarkeit



Verfügbarkeit



Authentizität

- Ziel kann durch Maßnahmen zur Authentisierung erreicht werden.

→ Welche Authentisierungsmethode?



Wissen
(z.B. Passwort)

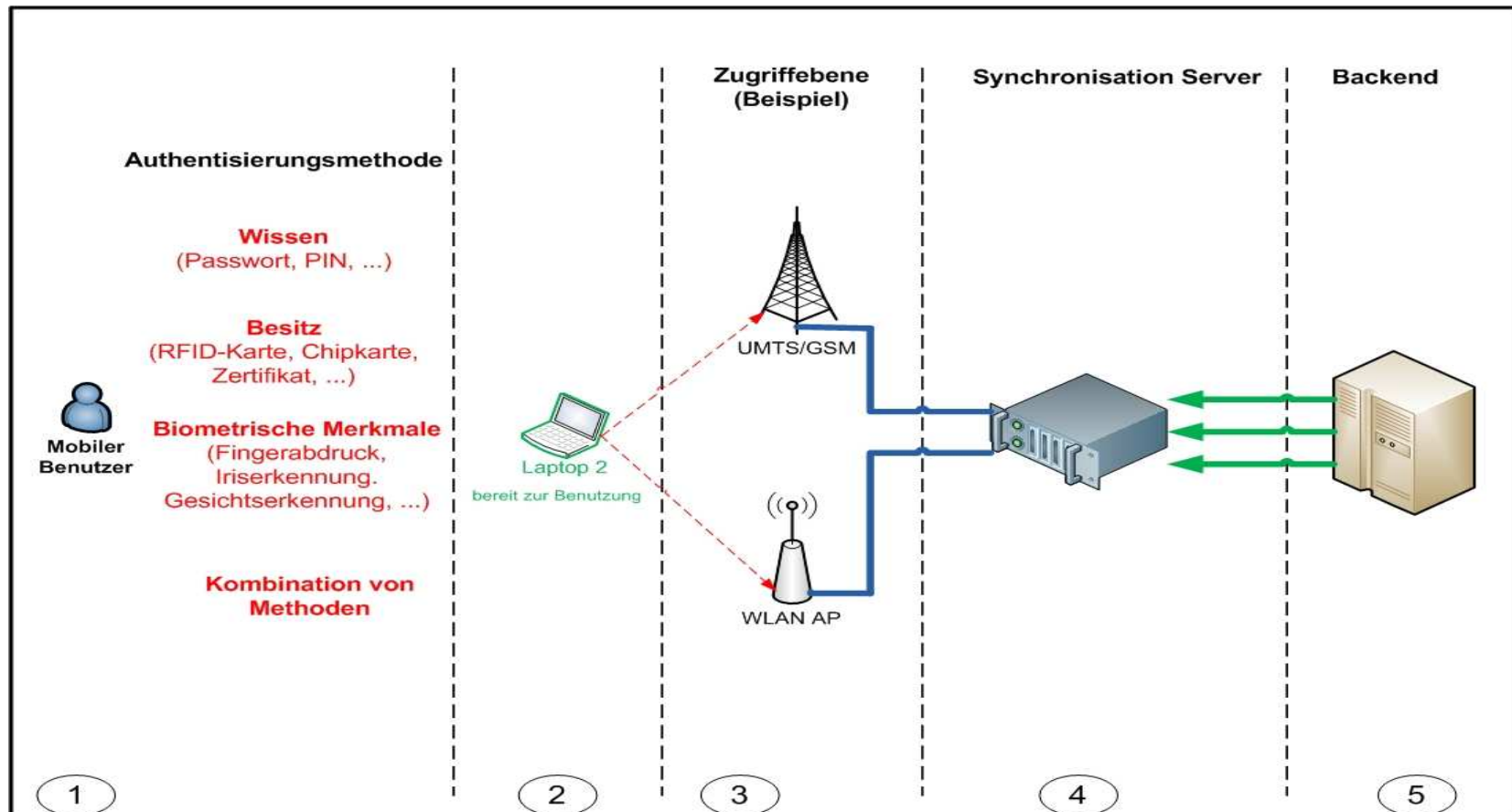


Besitz
(z.B. Chipkarte)



Biometrie
(z.B. Fingerabdruck)

Authentisierung



Authentisierung durch Wissen

- z.B. Passwortverfahren
- Am häufigsten verwendet
- Keine zusätzliche Hardware erforderlich
- Kennwortrichtlinien beachten
- + einfache Verwaltung
- + geringen Kosten
- Weitergabe
- Vergesslichkeit
- Erraten oder Herausfinden der Zugangsdaten durch Brute-Force- oder Dictionary-Attacken relativ einfach

Authentisierung durch Besitz

- z.B Chipkarte
- Keine Überprüfung des Besitzers sondern des Gegenstandes
 - Entwenden
 - Verlust
 - Duplizierung

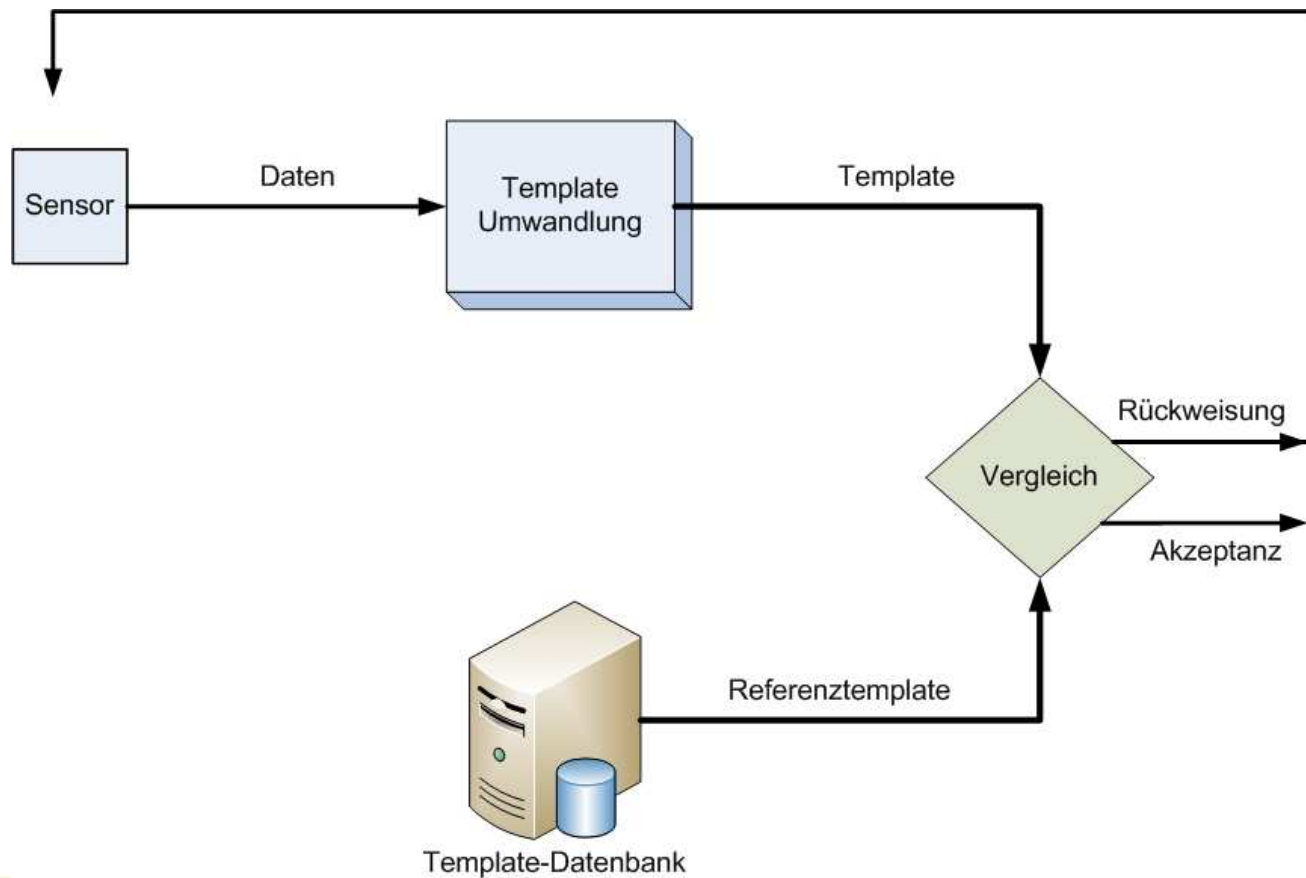
Biometrische Authentisierung

- Für den höheren Schutzbedarf verwendet
- Authentisierung anhand biologischer Merkmale
 - z.B Fingerabdruck, Iris, Gesicht, Stimme, ...

- Ablauf:
 - Registrierung (Enrolment)
 - Referenzdaten bilden (Template)
 - Vergleich (Matching)

- Aufnahme unter geänderten Rahmenbedingungen

Biometrische Authentisierung



Biometrische Authentisierung

- Vorteile:
 - Fälschung ist schwierig
 - Verlust eher selten
 - Person und ihre Daten untrennbar
- Nachteile:
 - Erkennungsprobleme bei Veränderung des Merkmals
 - Fehlerraten zu hoch
 - Hohe Kosten für die Einrichtung von biometrischen Systemen sind hoch

Sichere Authentisierung

- Kombination aus dreien Methoden
 - Zwei-Faktor-Authentisierung
 - Chipkarte + Passwort
 - Fingerabdruck + Passwort
- Eingebaute biometrische Lesegeräte + TPM-Module

Fazit

- Wearable: mehr Mobilität
- Unterstützung der Benutzer
 - Kontextsensivität
- Sicherheitskonzept erforderlich

Danke für Ihre Aufmerksamkeit

Quellangaben

- <http://www.bsi.bund.de/fachthem/biometrie/einfuehrung.htm>
- Eckert, Claudia: IT-Sicherheit – Konzepte, Verfahren, Protokolle, Oldenbourg Verlag München Wien, 4. Auflage, 2006
- Gerhard Tröster, Wearable Computing Lab, ETH Zürich