Fachhochschule Gelsenkirchen

Location Based Security
→Ansätze für ein Stufenkonzept

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
https://www.internet-sicherheit.de

if(is) internet-sicherheit.

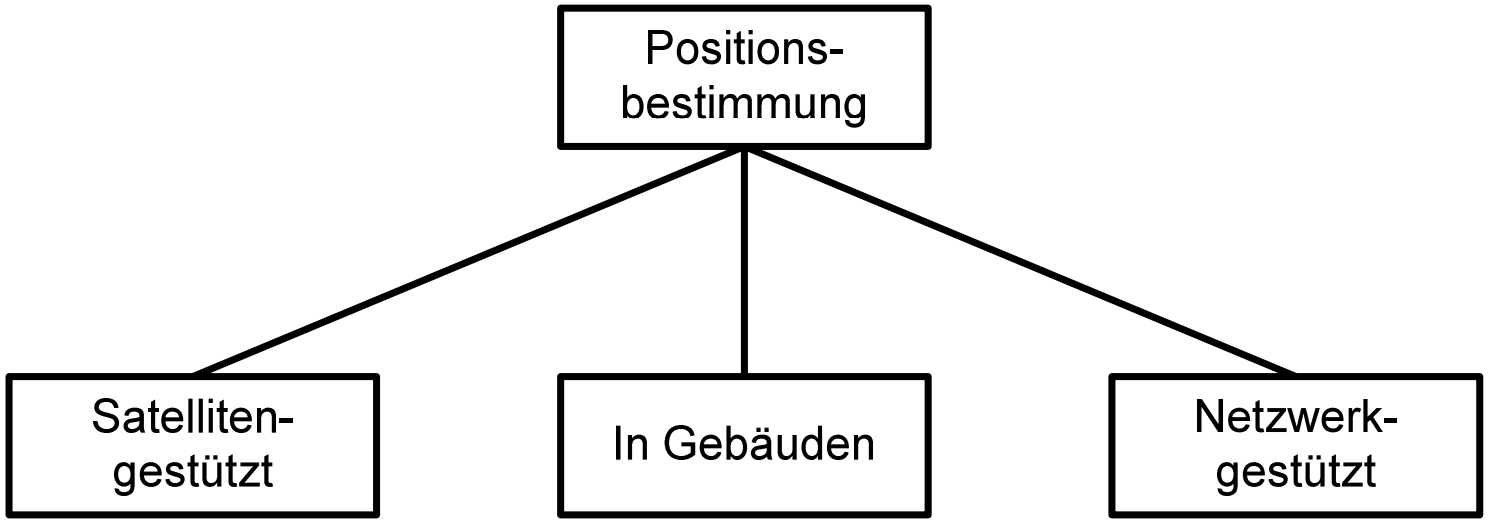
Inhalt

- **Konzepte der Positionsbestimmung**
- **Ortsabhängige Zugriffsrechte für (mobile) Geräte**
- **DRM für ortsabhängige IT-Sicherheit**
- **Architektur und Stufenkonzept**
- **Anwendungsszenarien und Ausblick**

Inhalt

- **Konzepte der Positionsbestimmung**
- Ortsabhängige Zugriffsrechte für (mobile) Geräte
- DRM für ortsabhängige IT-Sicherheit
- Architektur und Stufenkonzept
- Anwendungsszenarien und Ausblick

Positionsbestimmung
→ Unterschiedliche Technologie



GPS, Galileo, usw.

- Recht hohe Genauigkeit (GPS: 25 Meter, Galileo: 4 Meter)
- Weltweite Verfügbarkeit
- Positionieren in Gebäuden/Hochhaus-schluchten nur sehr schwer möglich

Infrarot, Ultraschall, Funk, WLAN, Bluetooth aber auch GPS

- Genauigkeit: Bis zu 10 cm, z.B. Ultraschal

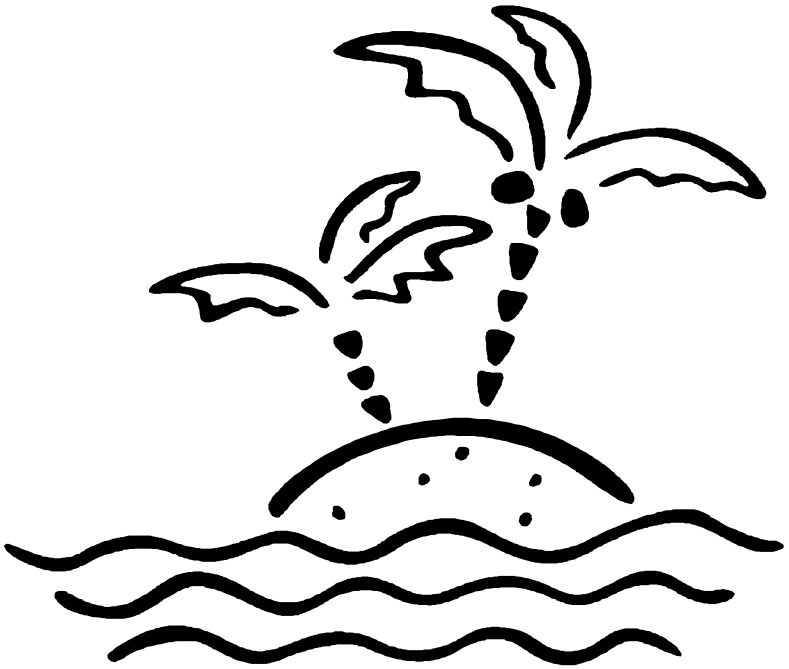
(GSM, UMTS, WLAN, Wimax, …)

- Genauigkeit hängt von den Zellen ab (50 m bis 35 km)
- in der Stadt 50-1000 m,
- auf dem Land >10 km (geht aber auch von 50-120 m)
- WLAN: Es gibt keine umgesetzten und einheitliche Verfahren
- WLAN: Genauigkeit 1,5 bis 10 Meter

Inhalt

- Konzepte der Positionsbestimmung
- **Ortsabhängige Zugriffsrechte für (mobile) Geräte**
- DRM für ortsabhängige IT-Sicherheit
- Architektur und Stufenkonzept
- Anwendungsszenarien und Ausblick

Sichere Umgebungen
→ Definierte und gesicherte Zone

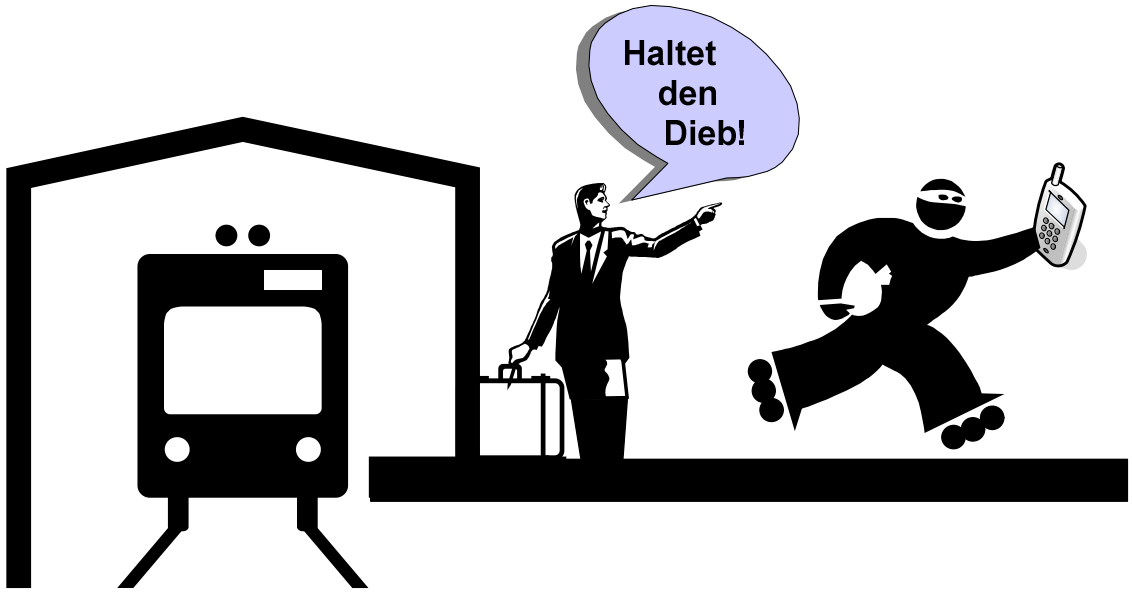


- **Einsame Insel:**
  - Keine „Fremder“ kann auf das mobile Gerät zugreifen

- **Eigenes Büro:**
  - Abschließbares Büro
  - Alleine mit dem Rechnersystem, dessen Daten und den Diensten

Mobile Anwendungen
→ Zusätzliche Gefahren

- Ein Angreifer kann sehr leicht die Sicht auf die Aktivitäten bekommen, wenn in der Öffentlichkeit gearbeitet wird.



- Der Diebstahl von mobilen Geräten in öffentlichen Umgebungen ist sehr viel leichter.

Ortsabhängige Zugriffsrechte für (mobile) Geräte

- Mobile Geräte befinden sich in **ständig wechselnden unsicheren Umgebungen**, wie Flughäfen, Bahnhöfen und sonstige öffentlichen Plätzen.
- Immer **wertvollere Daten und Dienste** stehen auf mobilen Geräten zur Verfügung.
- Aufgrund ihrer Mobilität sind sie außerdem **anfälliger für Angriffe** als herkömmliche stationärer Rechnersysteme, wie PC-Arbeitspläze im eigenen Büro.

- **Location Based Security (LBS)** bedeutet:
  - **Zugriffsrechte bei Anwendungen mit hohem Schutzbedarf** nicht nur
  - aufgrund von der **Identität und Authentizität des Benutzers** zu erteilen,
  - sondern auch den jeweiligen **Aufenthaltsort des Benutzers** für seine Möglichkeiten und Rechte auf Daten zuzugreifen und Dienste zu nutzen zu berücksichtigen.

Inhalt

- Konzepte der Positionsbestimmung
- Ortsabhängige Zugriffsrechte für (mobile) Geräte
- **DRM für ortsabhängige IT-Sicherheit**
- Architektur und Stufenkonzept
- Anwendungsszenarien und Ausblick

Digital Rights Management (DRM)
→ Übersicht

- Technische Maßnahmen, wie **kryptographische Sicherung der Daten**, zur **Durchsetzung von Nutzungsregeln** für Inhalte

- *DRM ist im Konsumentenmarkt kontrovers diskutiert (informationelle Selbstbestimmung vs. Eigentumsrechte der Urheber)*

- **DRM im Businessumfeld bringt nur positive Aspekte:**
  - **Sorgt für eine Durchsetzung von Datenschutzbestimmungen**
  - **Verbessert die Geheimhaltung von Informationen**
  - **Setzt Rechte auf mobilen Geräten um**

- **DRM benötigt ein sicheres Soft- und Hardwarefundament (Trusted Computing), um vertrauenswürdig implementiert werden zu können!**

Mobile Anwendungen
→ Idee DRM

- Nutzung von **Digital Rights Management (DRM) Funktionalitäten** und **Trusted Computing Technologie** auf einem mobilen Endgerät, zur sicheren Mobilisierung von Prozess- und Wertschöpfungsketten.

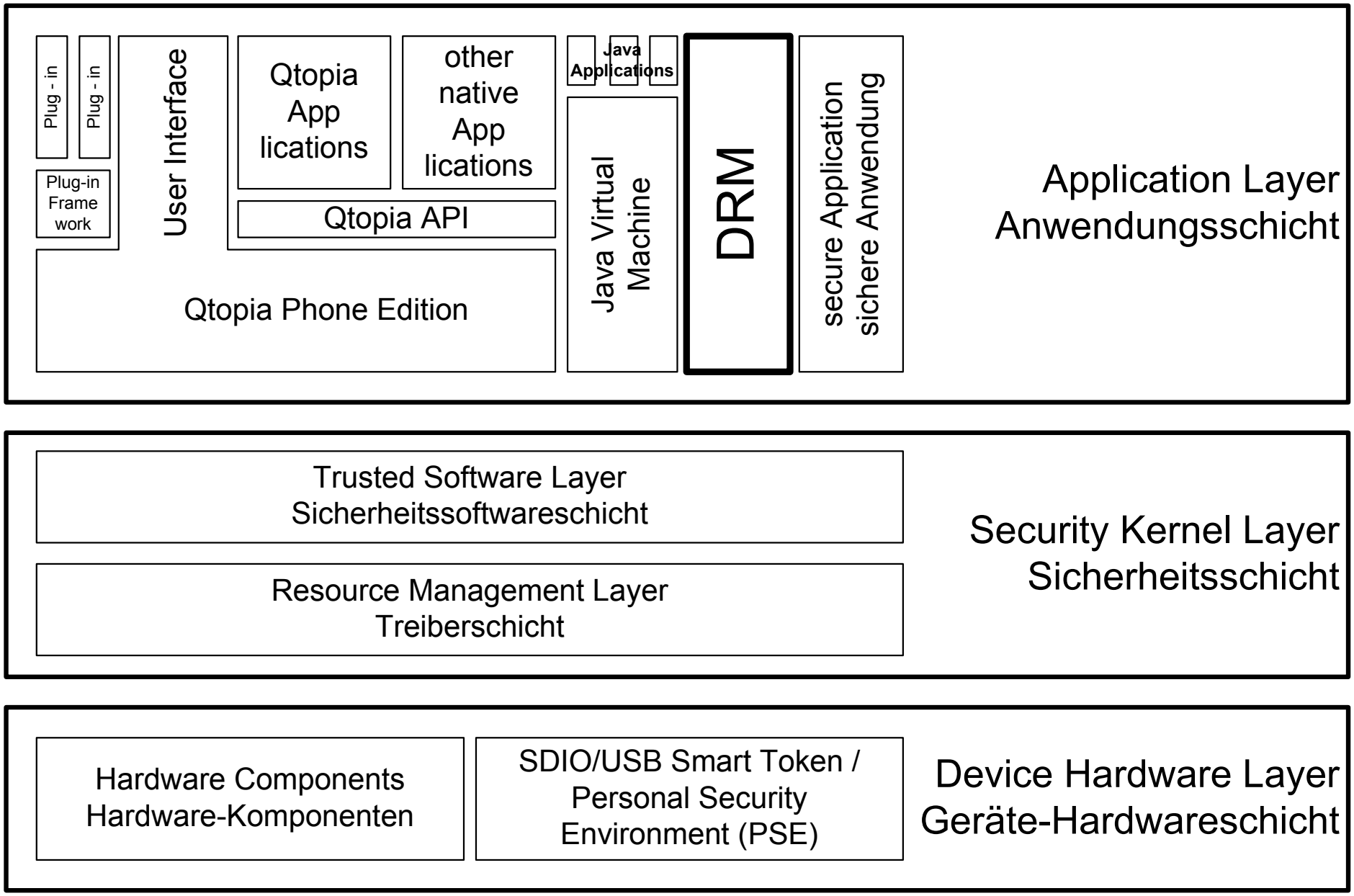
- **Besondere Sicherheitsziele:**
  - Durchsetzen von datenschutzrechtlichen Aspekten
  - Sicherstellen der Vertraulichkeit von geheimen Informationen
  - Verbindlichkeit für das Handeln des mobilen Benutzers
  - Überprüfbare Integrität und Herkunft der Information und IT-Systeme
  - Durchsetzen von Nutzungsbeschränkungen (Objekte, Funktionen, usw.)

Inhalt

- Konzepte der Positionsbestimmung
- Ortsabhängige Zugriffsrechte für (mobile) Geräte
- DRM für ortsabhängige IT-Sicherheit
- **Architektur und Stufenkonzept**
- Anwendungsszenarien und Ausblick

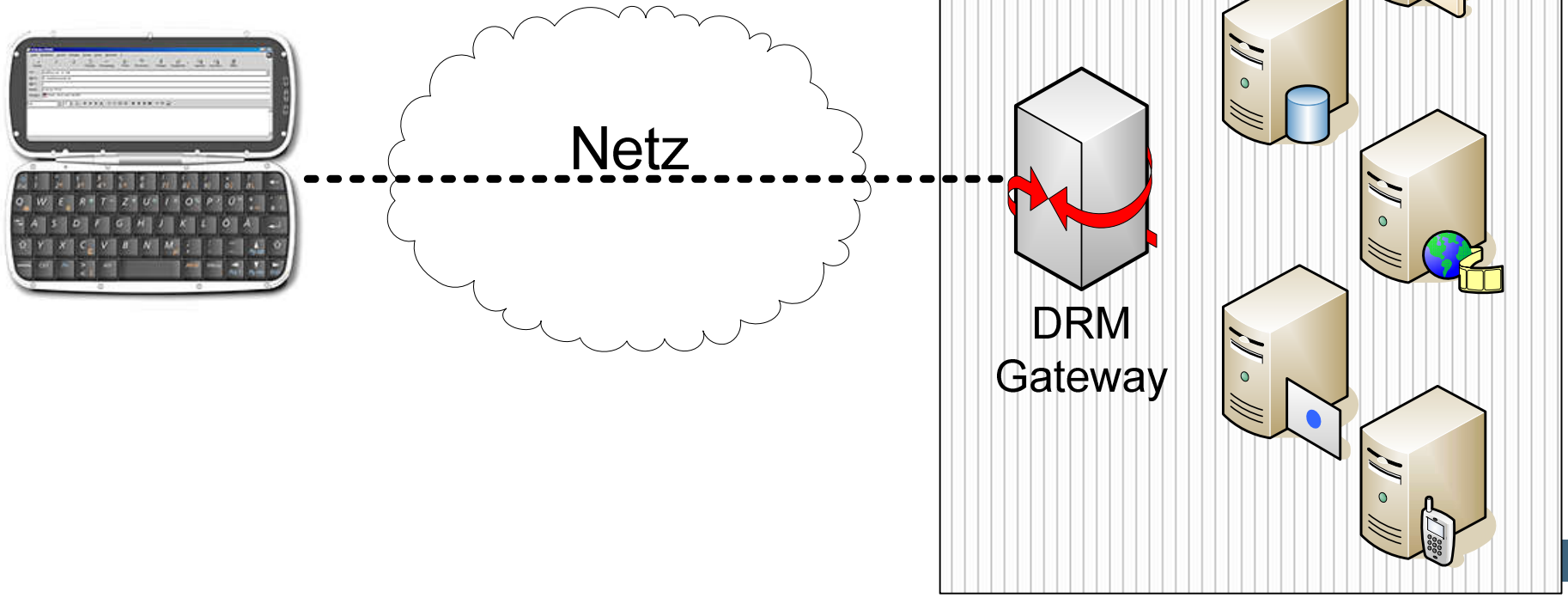
Analogie
→ Sicherheit für den mobilen Mitarbeiter

Architektur



Prozesseinbindung
→ DRM-Gateway

- **Idee**
  - Wir bauen ein **DRM-Gateway**, welches die Verschlüsselung des Anhanges in der Prozesskette durchsetzt.
  - Die **Policy** kann im Text als **MetaSprache** eingegeben werden.
  - Dateien ohne Meta-Daten werden nicht auf mobile Geräte übertragen.

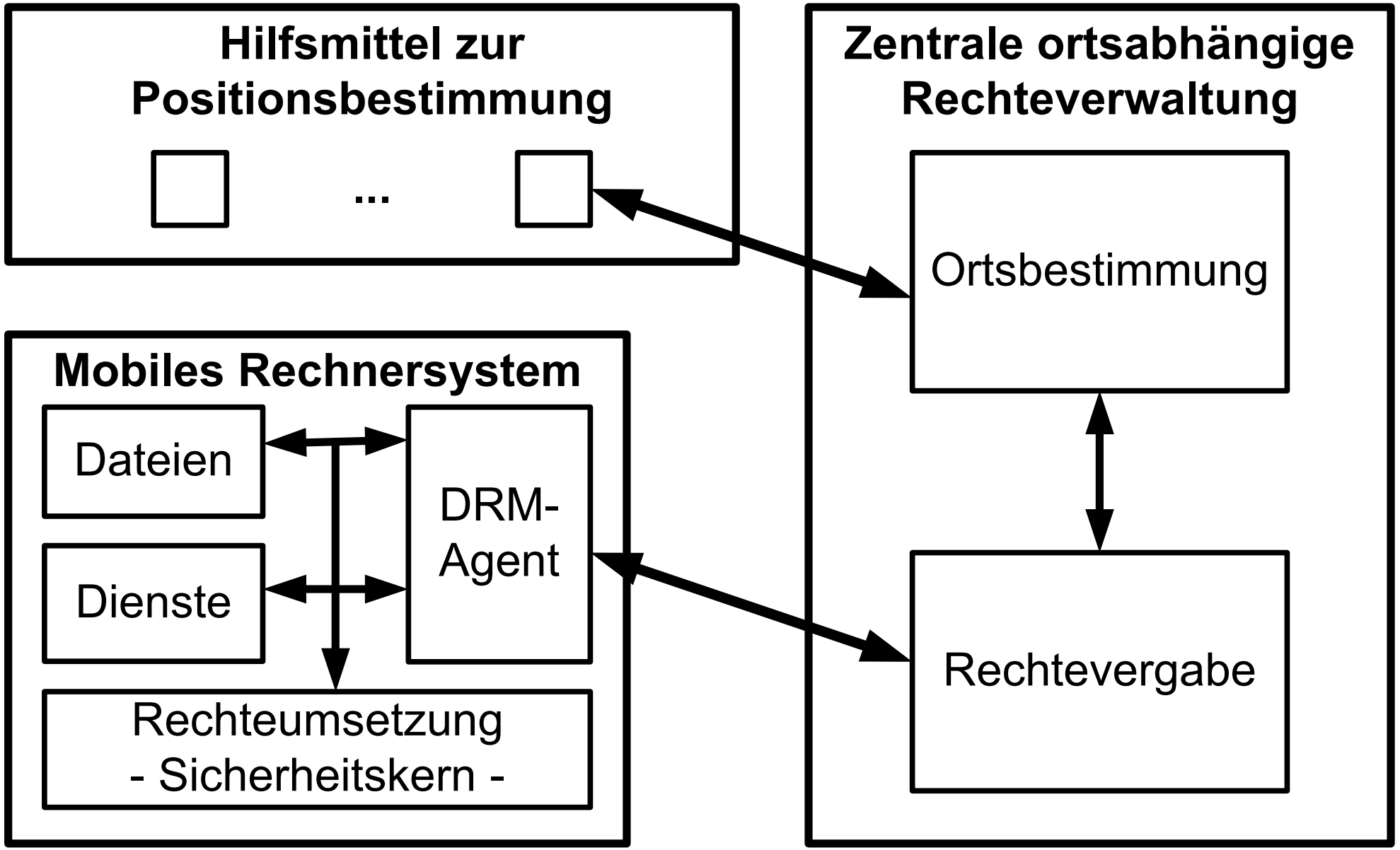


Prozesseinbindung
→ Ablaufbeispiel

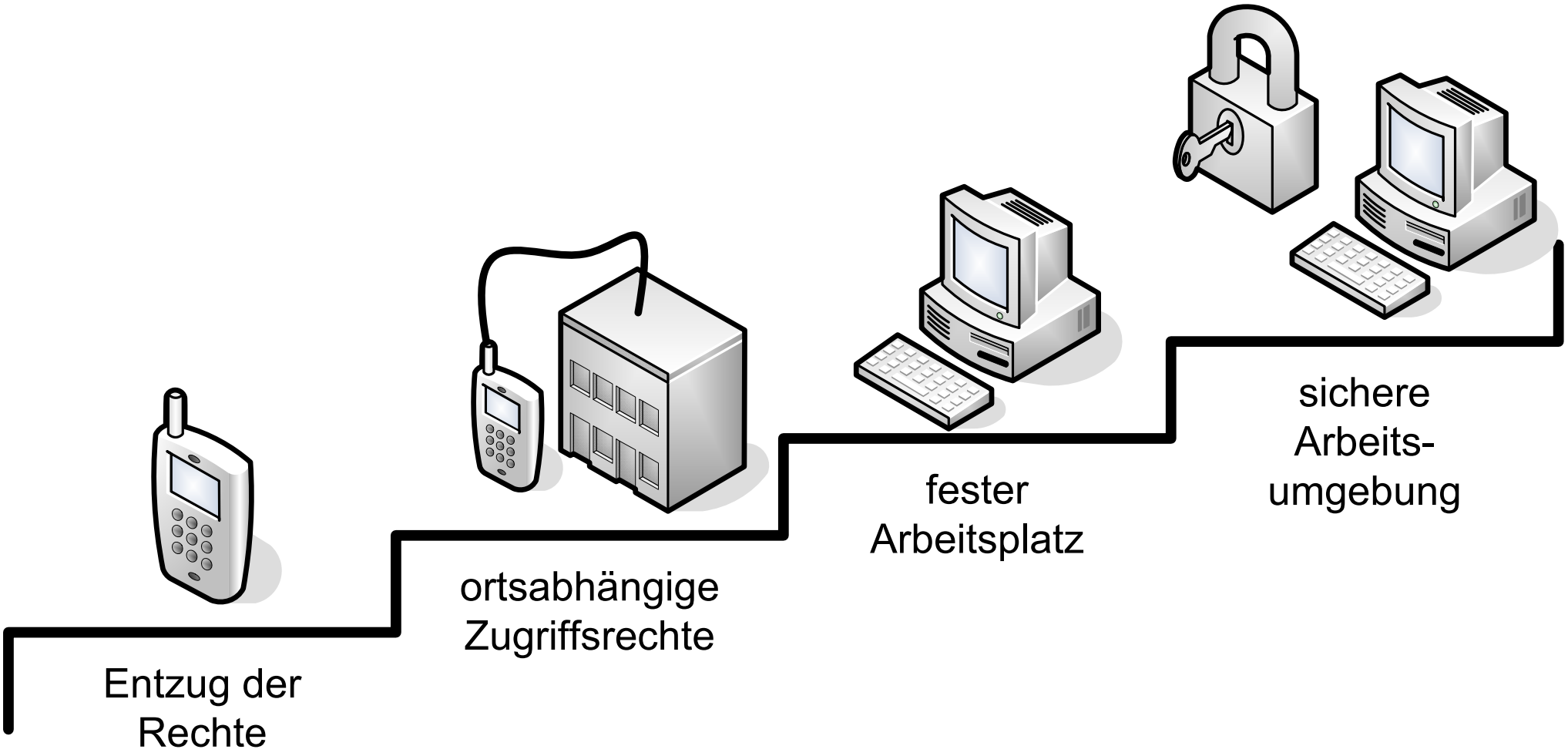
- **Alle Objekte werden mit Hilfe von DRM-Funktionen gesichert**
  - Verschlüsselung des Objekts ⟶ DRM
  - Rechte über Policy und abhängig von:
    - einer attestierten Geräteumgebung ⟶ Trusted Computing
    - Anwendungen (E-Mail, Word, EXCEL, usw.) ⟶ DRM
    - Aktionsrechten (Schreiben, Lesen, usw.) ⟶ DRM
    - Möglicherweise vom Ort über WLAN, GSP, usw. ⟶ LBS

- **Beispiel: Word-Dokument**
  - Darf nur drei Mal gelesen und gelöscht werden
  - Kein Schreiben oder Verändern
  - Kein Drucken
  - Kein Kopieren auf USB, usw.
  - Kein Versenden per E-Mail, usw.

Prozesseinbindung
→ Location Based Security



Location Based Security
→ Stufenkonzept



Inhalt

- Konzepte der Positionsbestimmung
- Ortsabhängige Zugriffsrechte für (mobile) Geräte
- DRM für ortsabhängige IT-Sicherheit
- Architektur und Stufenkonzept
- **Anwendungsszenarien und Ausblick**

Anwendungsszenarien

- **Customer Relation Management Systems**
  - Befindet sich der Mitarbeiter beim Kunden A, kann er nur auch auf die Daten des Kunden A zugreifen!

- **Ambulante Pflege Dienste**
  - Nur Zugriff auf Stamm- und Diagnosedaten der speziellen Patienten!

- **„stationärer“ Rechner verlässt die sichere Zone**
  - Reparaturmaßnahme oder Diebstahl
  - Keine Zugriff auf Daten und Dienste außerhalb der definierten und gesicherten Zone

Ausblick

- **„Location Based Security“** eine sehr gute Möglichkeit, mobile Geräte in Arbeitsprozesse einzubinden und die geforderte Sicherheit in angemessener Art und Weise zu erreichen.

- Das vorgestellte Konzept auf der Basis von **Trusted Computing** und **DRM** in Verbindung mit der **Lokalisierung des Rechnersystems und seiner Umgebung** gibt eine flexible Möglichkeit, auf die verschiedenen Anforderungen geeignet reagieren zu können.

Fachhochschule Gelsenkirchen

Location Based Security
→Ansätze für ein Stufenkonzept

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
https://www.internet-sicherheit.de

if(is) internet-sicherheit.