Sicherheitsarchitektur für mobile spontan vernetzte Geräte

Prof. Dr. Clemens Cap

Dipl.-Ing. Igor Sedov

FB Informatik

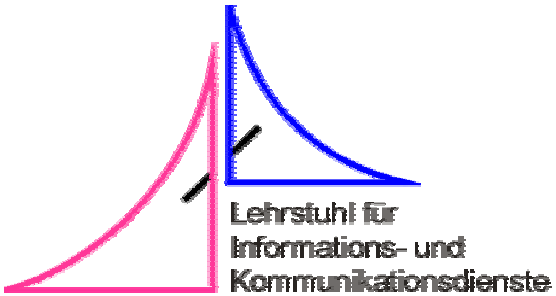
Institut für Technische Informatik

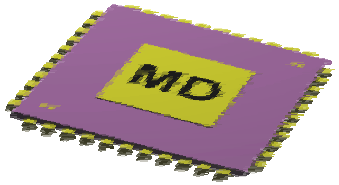
Prof. Dr. Dirk Timmermann

Dipl.-Ing. Marc Haase

FB Elektrotechnik u. Informationstechnik

Institut für Angewandte Mikroelektronik und Datentechnik





Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt - Ablauf des Vortrags...

1. Problemstellung
2. Spontane Vernetzung
3. Ziele des Projekts
4. Sicherheitsprobleme
5. Technologie
6. Realisation
7. Ausblick

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Spontane Vernetzung

Telefon

Modem

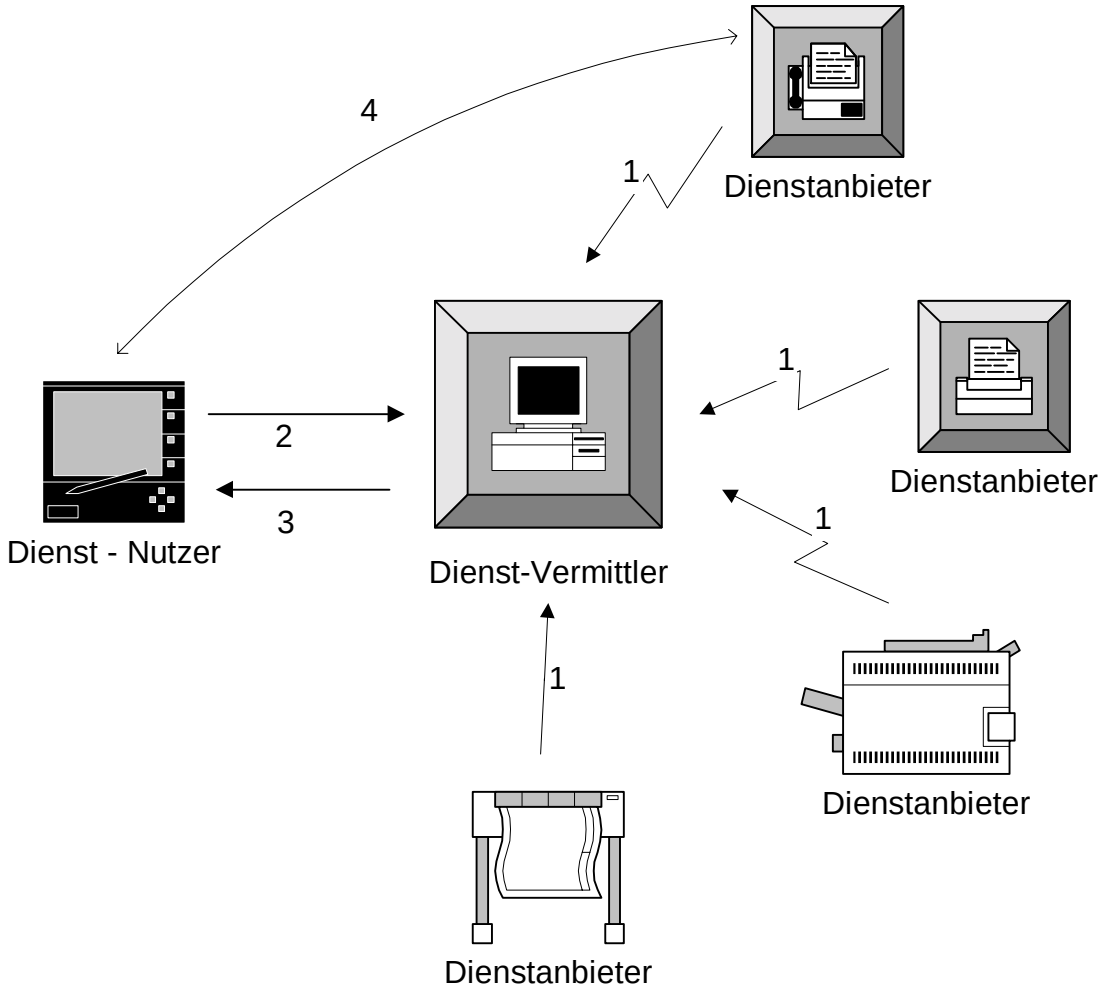
Fax Gerät

S/W Drucker

Photodrucker

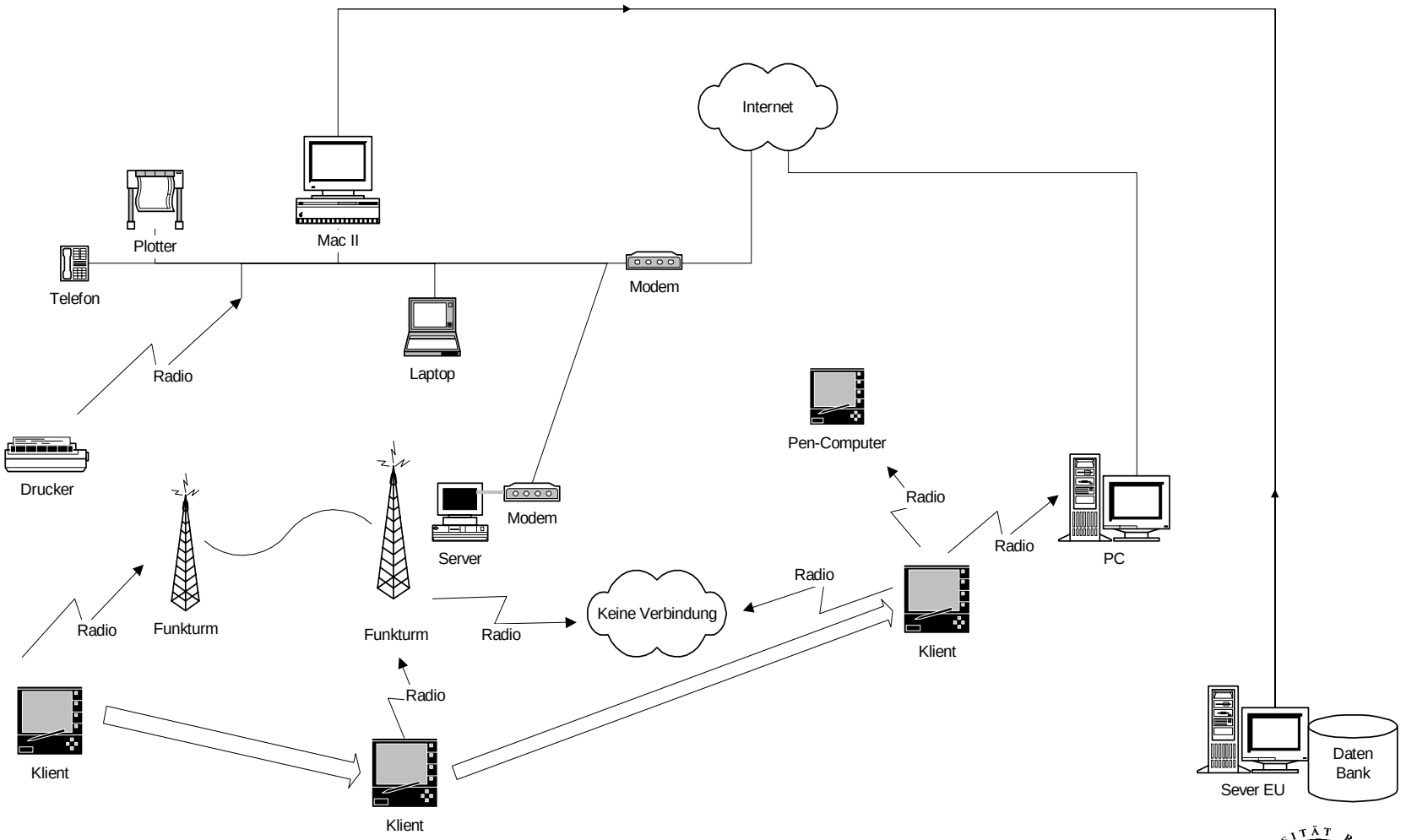
Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Spontane Vernetzung



Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Spontane Vernetzung



Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Ziele des Projektes

- Konzeption und Realisation der Architektur
- Angriffsszenarien und entsprechende Lösungsmodelle
- Authentifikation des Benutzers gegenüber seinem portablen Gerät über ein biometrisches Erkennungsverfahren
- Individuelle Anpassung des Sicherheitslevels für die Dienste

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Sicherheitsprobleme und Angriffsszenarien

- Besonderheiten der Radiowellen
- DA, Übertragungsmedium, Server, höhere Instanz
- Diebstahl und Klonung des DA
- Beschränkte Rechenleistung, Roaming

⇨ Verlust der Vertraulichkeit

⇨ Bedrohung der Datenintegrität

⇨ Denial-of-Service–Bedrohung

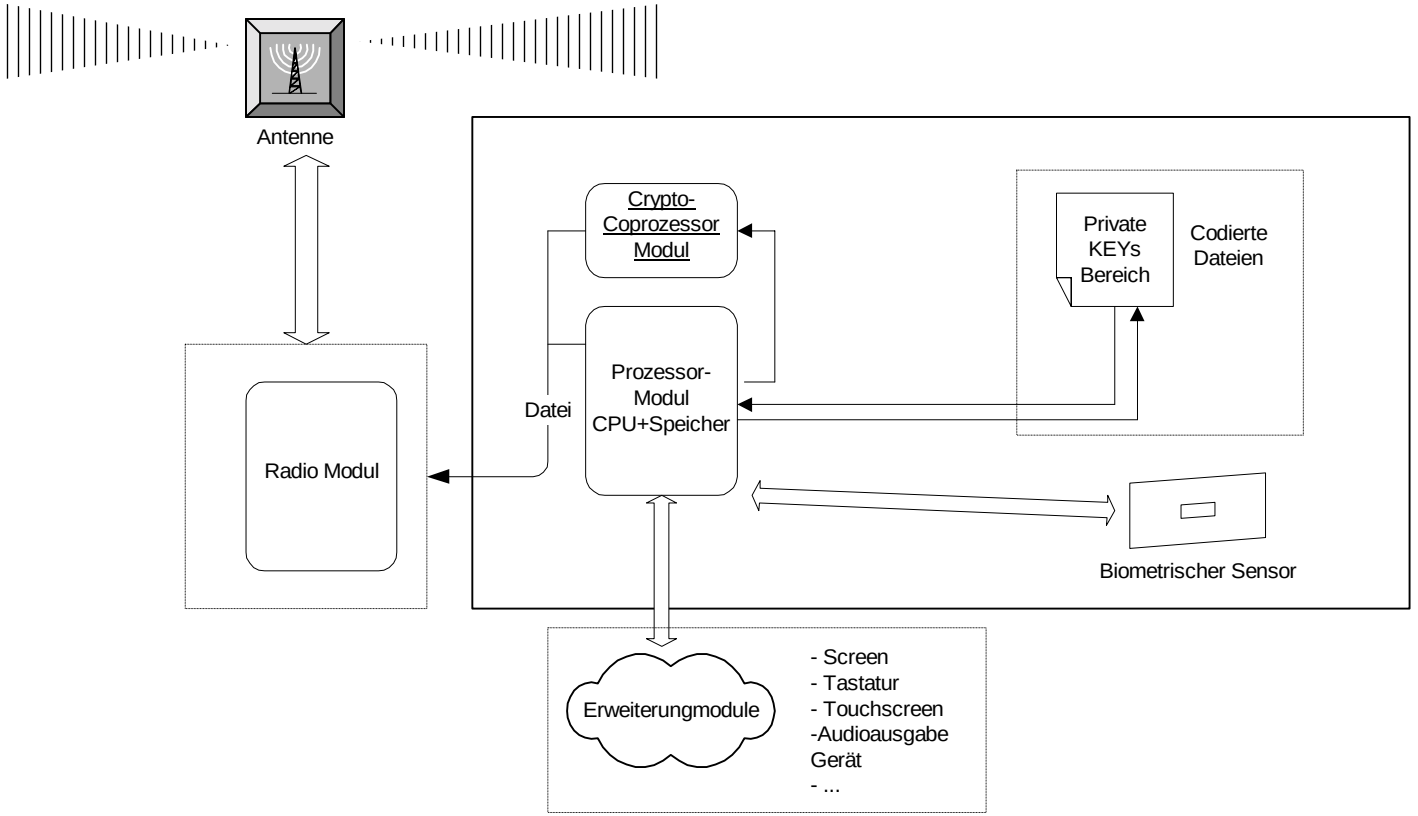
Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Realisation

1. Radiomodul
2. Crypto-Coprozessor Modul
3. Prozessor Modul
4. Biometrischer Sensor
5. Erweiterungsmodule

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Realisation



Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Radiomodul

Bluetooth

- Reichweite bis 100 m, point-to-point, point-to-multipoint
- Baugröße 10,2x140x1,6 mm. Übertragung durch Wände und andere nicht-metallische Objekte
- Weltweit lizenzfreier Funkfrequenzbereich ISM 2.4 GHz

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Mögliche Technologien

- Assynchronmodus maximal 721 Kb/s (57,6 Kb/s)
- Symmetrische Verbindung bis 432,6 Kb/s
- Bis 7 Slave + 1 Master → Pico-Netz
- „Frequency hopping spread spectrum“, 1600 mal pro sec.
- Sicherheitsverfahren und Fehlerkorrekturmethoden auf Bitübertragungsebene
- Authentifizierung 128 Bit
- Verschlüsselung von 8 bis 128 Bit

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

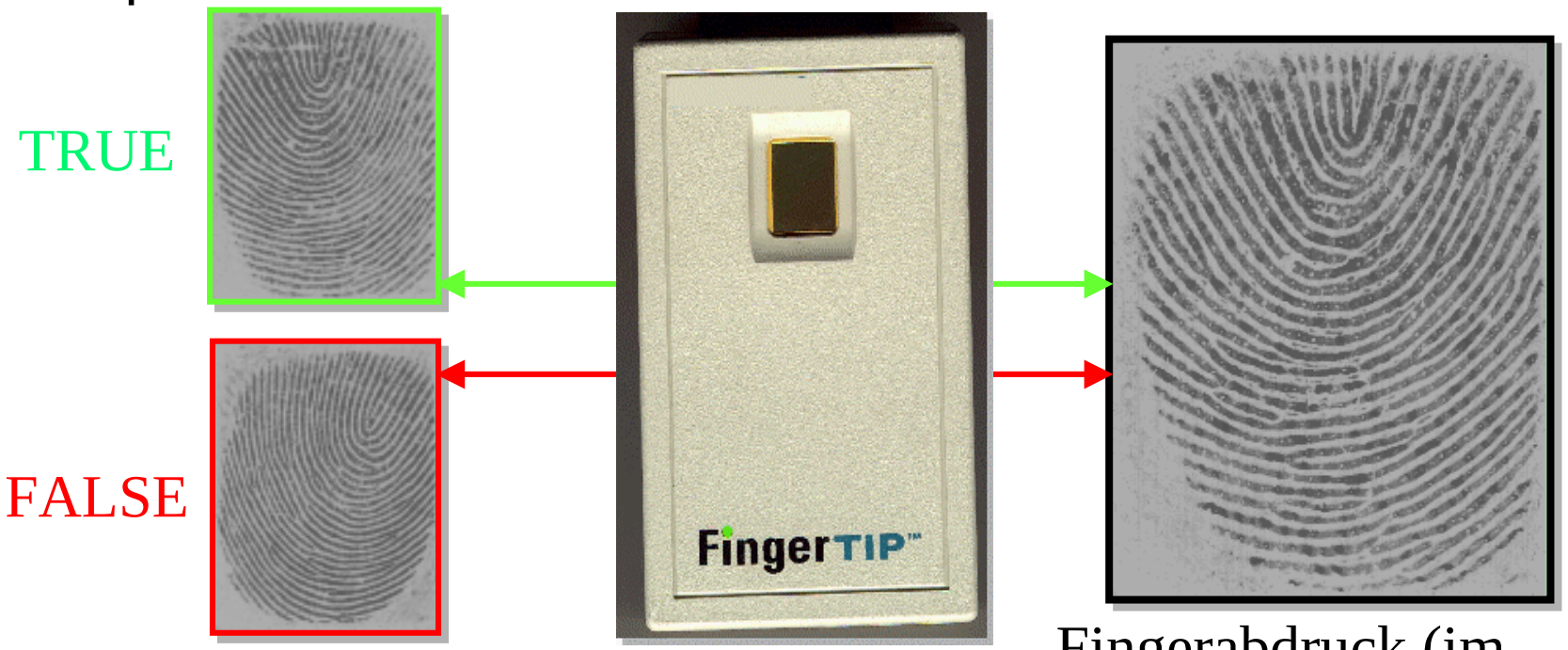
Infrarot

- Geschwindigkeit von 9600 Kb/s bis 4 Mb/s (16Mb/s)
- Nur Point-to-Point im Winkel bis 30°
- Reichweite 1-2 m
- Reflektierte Lichtwellen

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Mögliche Technologien

- Authentifikation des Nutzers gegenüber seinem portablen Gerät



Fingerabdruck (aktuell)

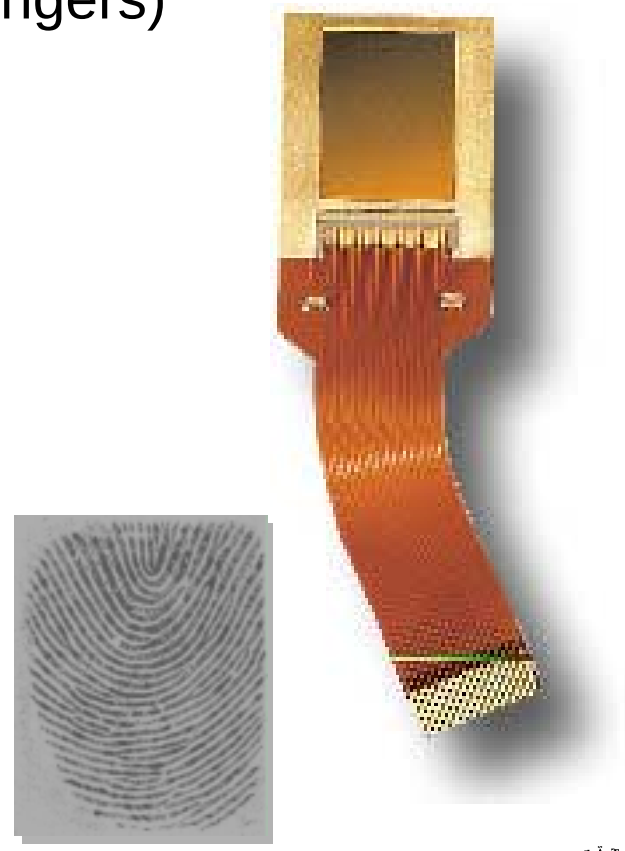
Verifikation (identische Fingerabdrücke?)

Fingerabdruck (im „Private Keys“ Bereich gespeichert)

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Fingerprint ID modul

- Minuzienvergleich (Merkmale des Fingers)
- Erkennungssicherheit
- Fälschungssicherheit
- Handhabung
- Speicherbedarf
- Sparsamer Stromverbrauch
- Datenschutz



Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

Drei Sicherheitsformen des Zugangs

- Sicherheitslevel 1: Keine Sicherheitsprozeduren
- Sicherheitslevel 2: Nur Authentifikation, Autorisation ist nicht erforderlich
- Sicherheitslevel 3: Sowohl Authentifikation, als auch Autorisation sind erforderlich

Trusted und Untrusted Devices

- Unterschied zwischen „Link Layer“ und „Application Layer“
- Autorisation des Nutzers gegenüber Gerät

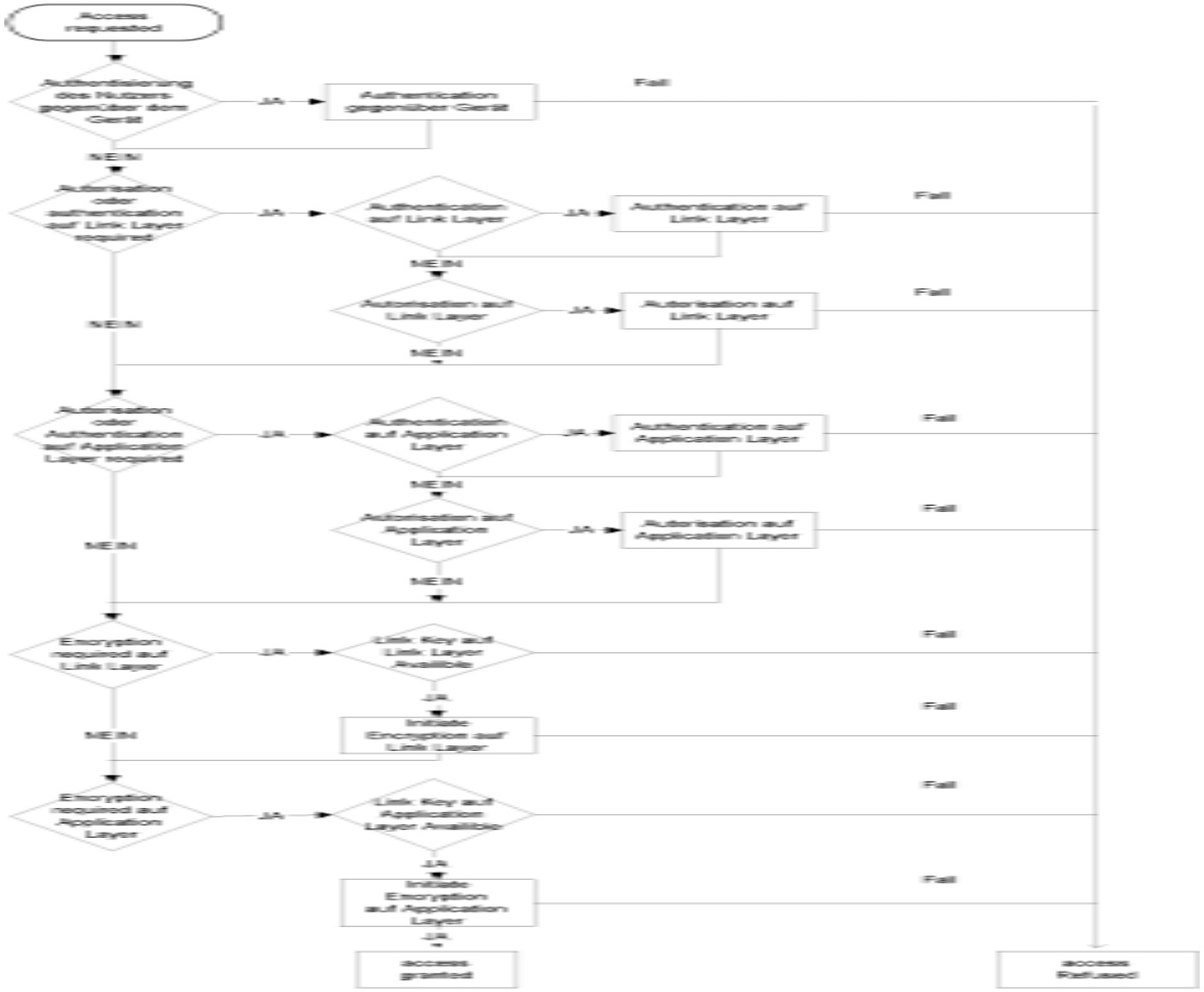
Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Realisation

Parameter	Größe
1. Service - Name	?
1. BD_ADDR - Die Adresse des Bluetooth Gerätes auf „Link Layer“	48 bit
2. BD_ADDR – Die Adresse des Gerätes auf „Application Layer“, wenn zusätzliche Authentifikation auf „Application Layer“ erforderlich ist	48 bit
3. Flag „Autorisation Required“ auf „Link Layer“	1 bit
4. Flag „Authentification Required“ auf „Link Layer“	1 bit
5. Flag „Autorisation Required“ auf „Application Layer“	1 bit
6. Flag „Authentification Required“ auf „Application Layer“	1 bit
7. Keys „Links Layer“	?
8. Keys „Application Layer“	?
10. Flag Authentifikation des Nutzers gegenüber dem Gerät	1 bit
11. Encryption Required	1 bit

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Realisation



Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de

DFG Projekt SPP - Problem Stellung

- Beispielszenarien:
  - Referenzszenario - Handel, Banken oder Versicherungen
  - Referenzszenario - Medizin
  - Referenzszenario - Produktionsprozeß

Dtim@e-technik.uni-rostock.de
Cap@informatik.uni-rostock.de