Proseminar Kryptographische Protokolle SS 2009

Bluetooth

Medin Imamovic

Inhalt

1 Einleitung

- Bluetooth – Technologie zur drahtlosen Kommunikation
- 1994 entwickelt von Ericsson
- Name – Wikingerkönig Harald Blatand (Blauzahn)
- 1998 Gründung der Bluetooth-SIG (Special Interest Group)
- Juli 1999 Veröffentlichung der Bluetooth Spezifikation Version 1.0

1.1Technische Grundlagen

- **Kommunikation:**

SCO *(Synchronous Connection Oriented)*

-leitungsvermittelt Kommunikation

-zur Übertragung von Sprachdaten

ACL *(Asynchronous Connection Less)*

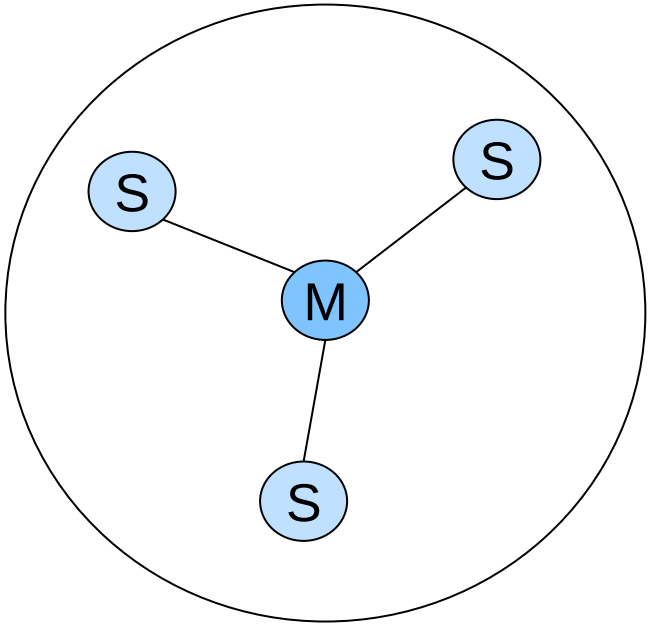
-paketvermittelte Kommunikation

-zur Übertragung aller anderen Daten

1.1 Technische Grundlagen

- **Bluetooth-Netze:**

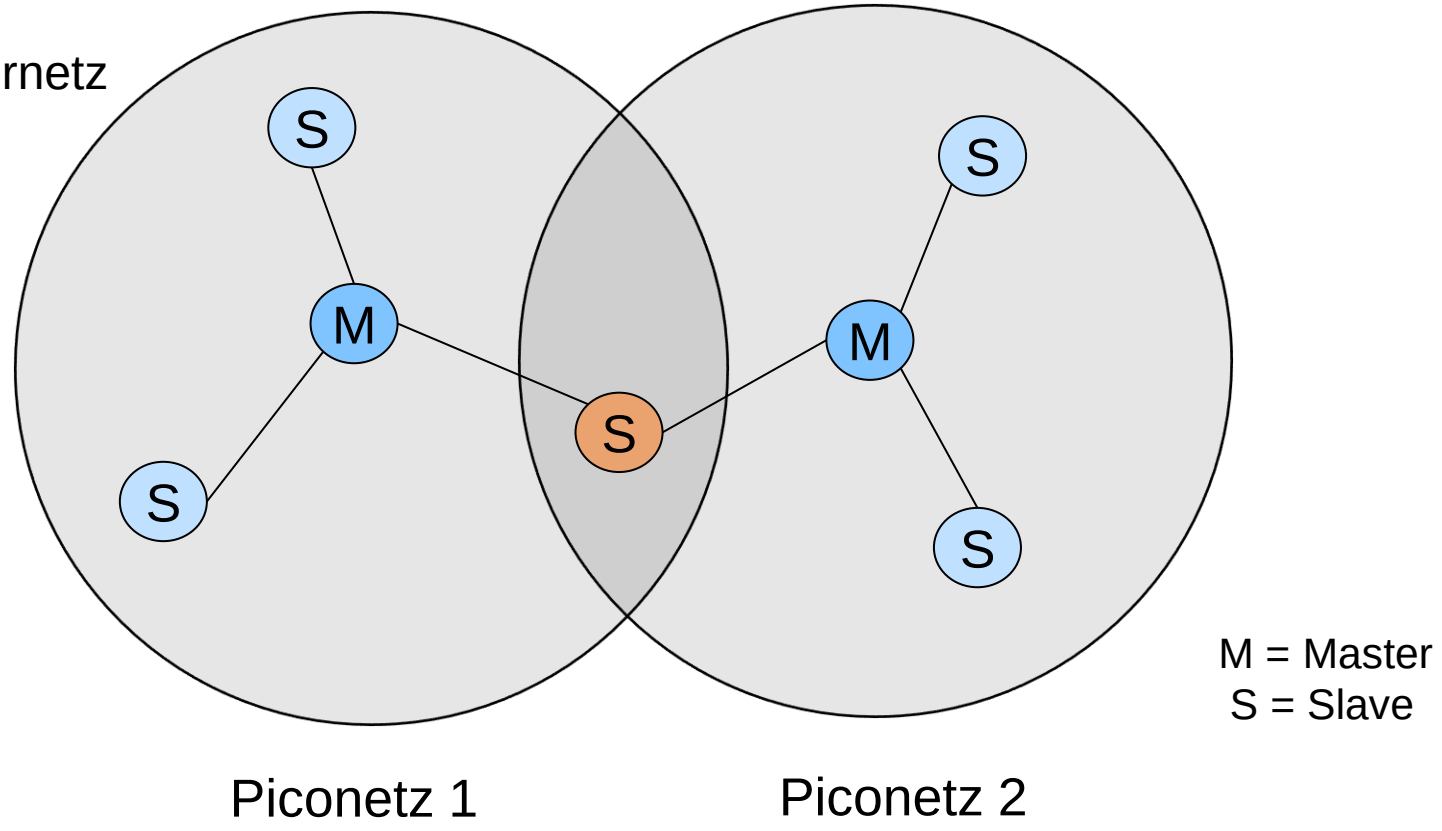
  -Piconetz



M = Master
S = Slave

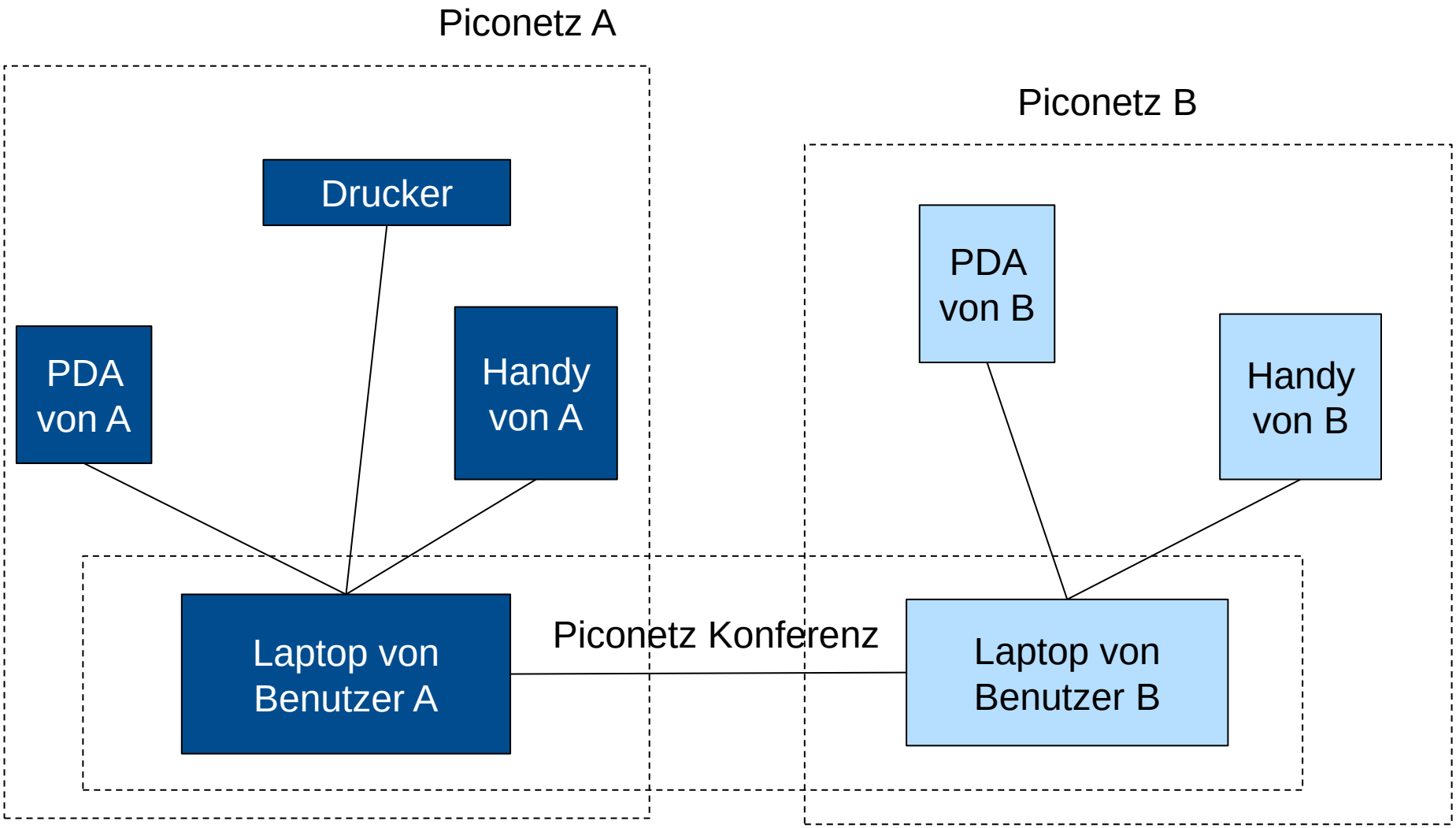
1.1 Technische Grundlagen

- Scatternetz



Scatternetz Beispiel

Abb. [Q1] S.863



Exkurs: ISO – OSI Schichtung

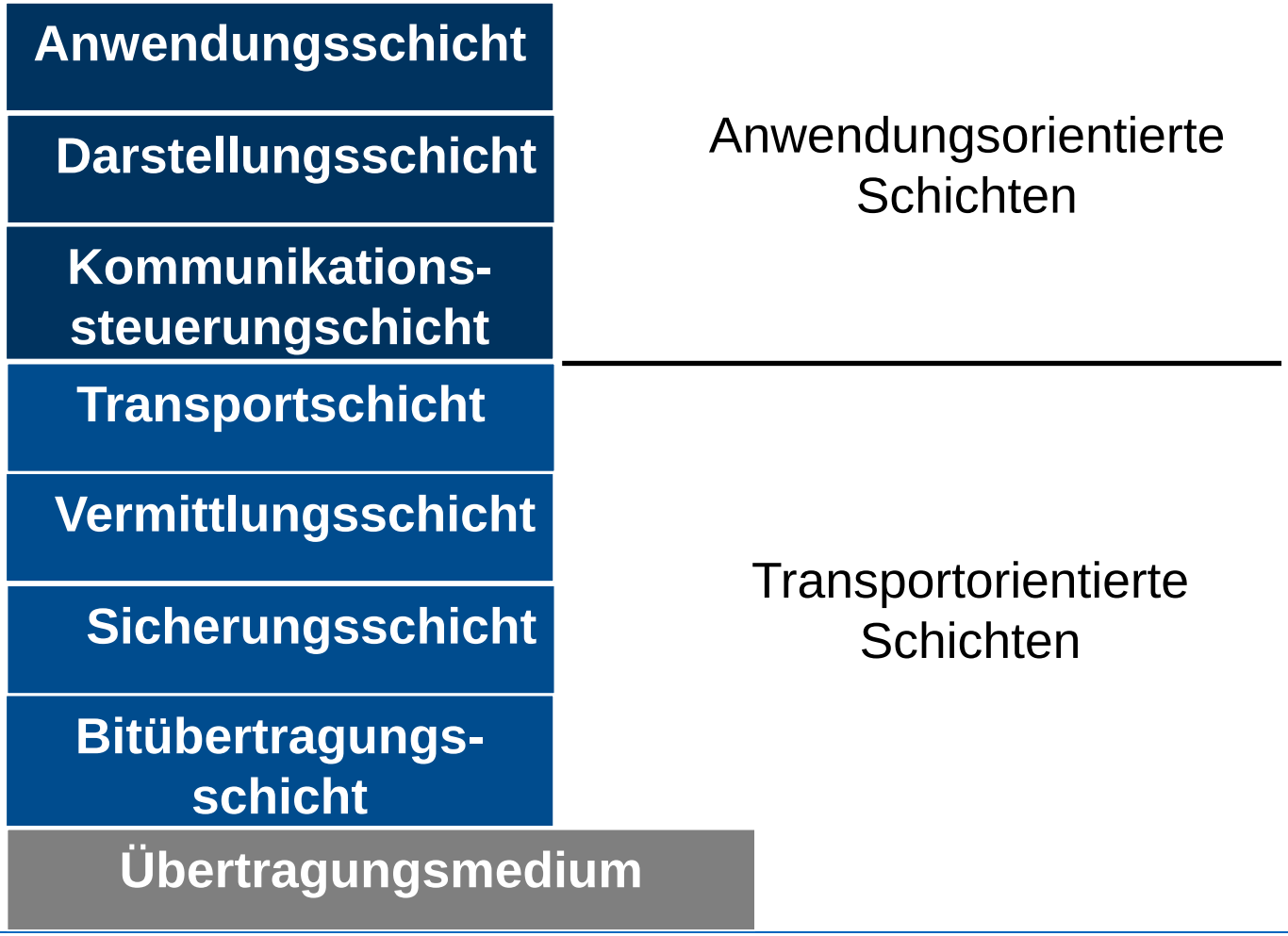


Abb. [Q3]

1.2 Protokollstack

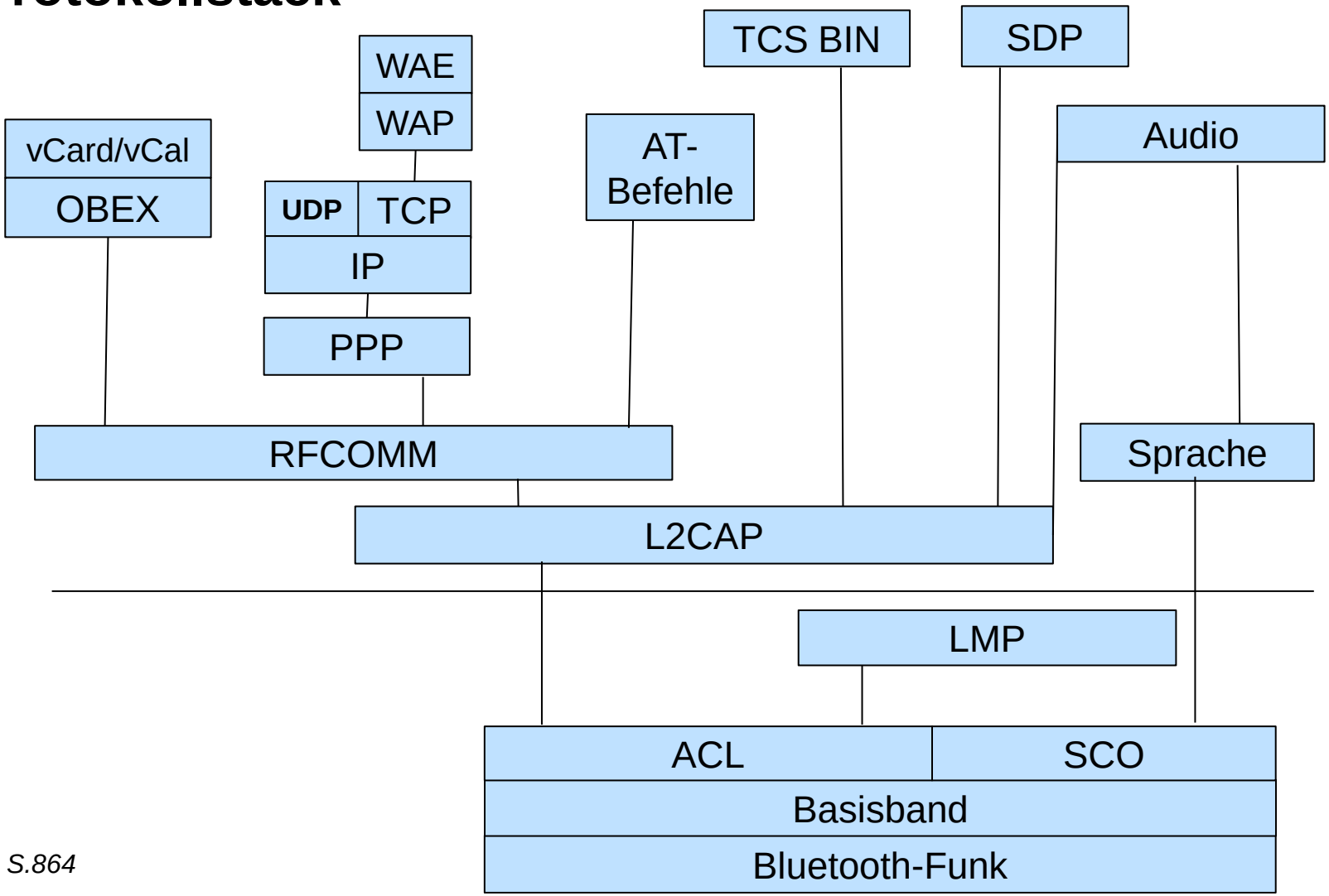


Abb. [Q1] S.864

2 Schlüsselmanagement

- Verbindungsschlüssel
  - Geräteschlüssel
  - Initialisierungsschlüssel
  - Kombinationsschlüssel
  - Masterschlüssel

Geräteschlüssel

- Besteht aus:

  - 128 Bit Zufallszahl
  - 48 Bit Geräteadresse BD_ADDR

- Wird im Speicher des Geräts abgelegt und in der Regel nicht mehr geändert

Initialisierungsschlüssel

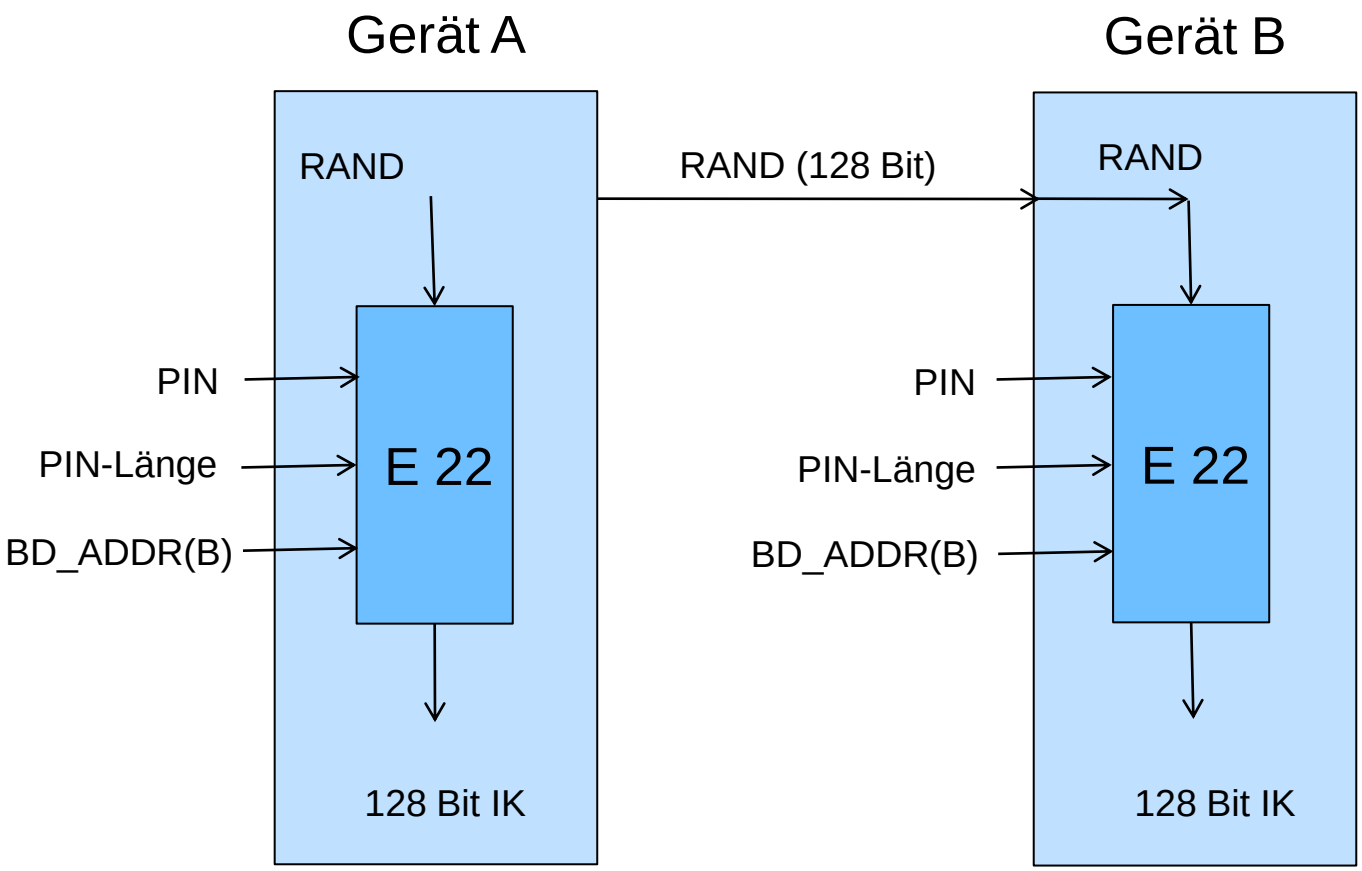
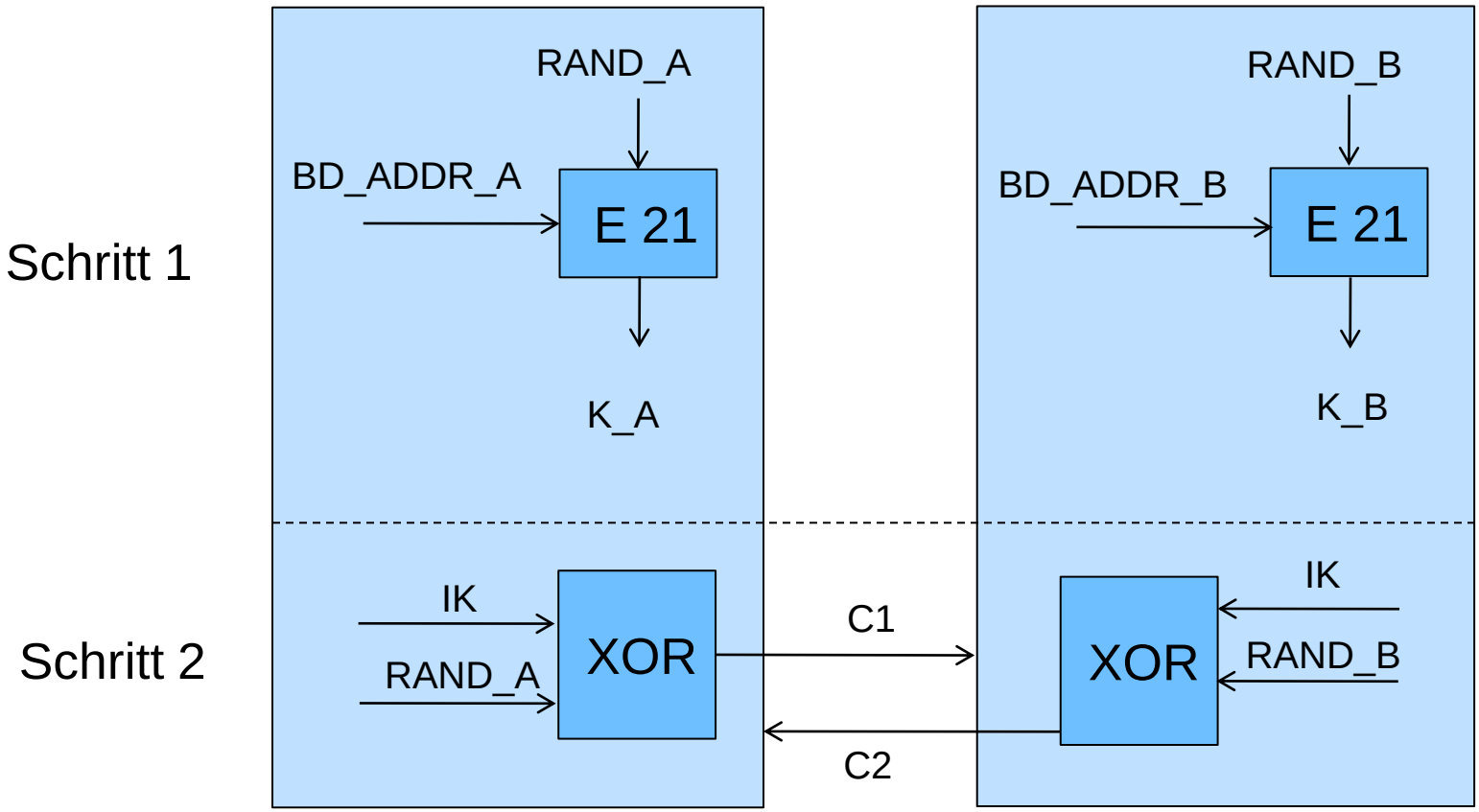


Abb. [Q1] S.874

Kombinationsschlüssel I



Kombinationsschlüssel II

Schritt 3

Schritt 4

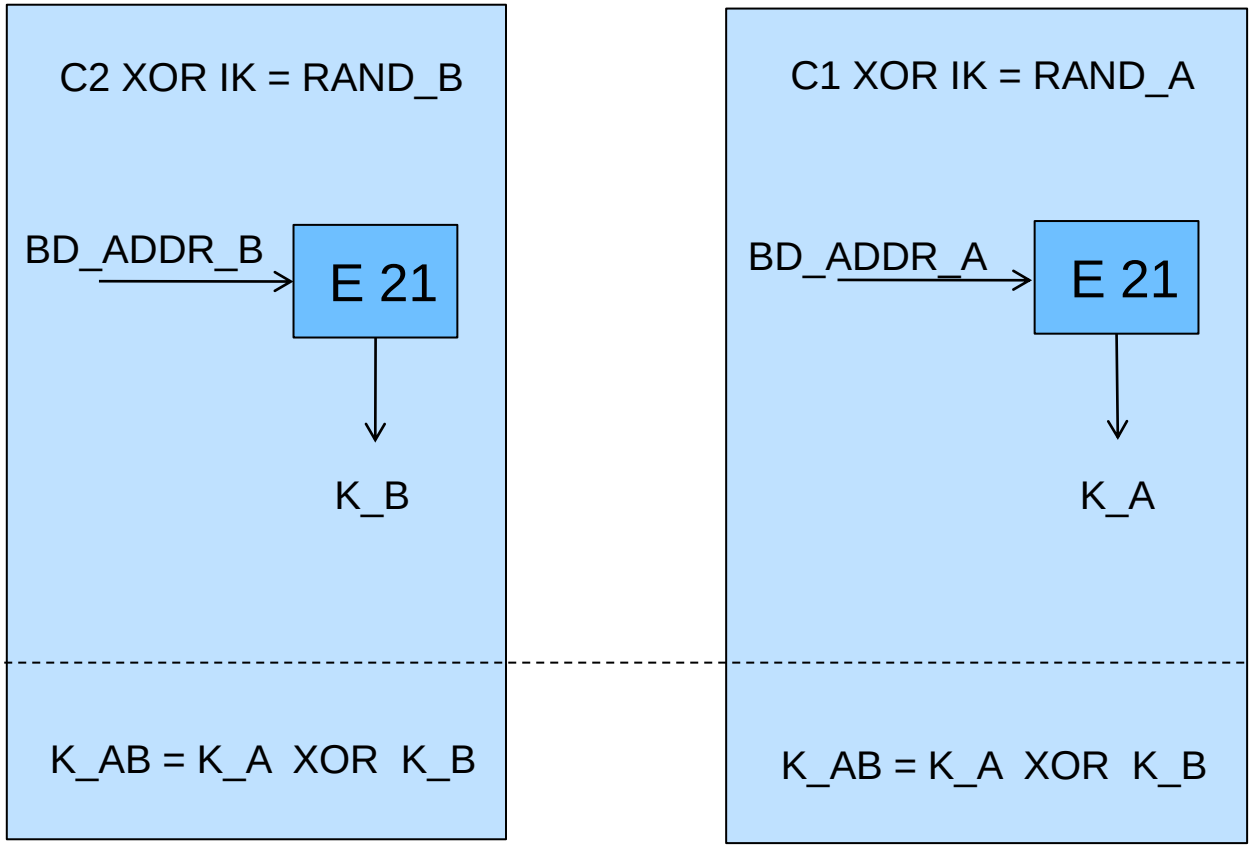


Abb. [Q1] S.875

Masterschlüssel

- Temporär
- Austausch von Informationen zu mehreren Empfänger
- Wird vom Master mittels E21 und zweier Zufallszahlen erzeugt
- Ist 128 Bit lang

2.1 Authentifikation

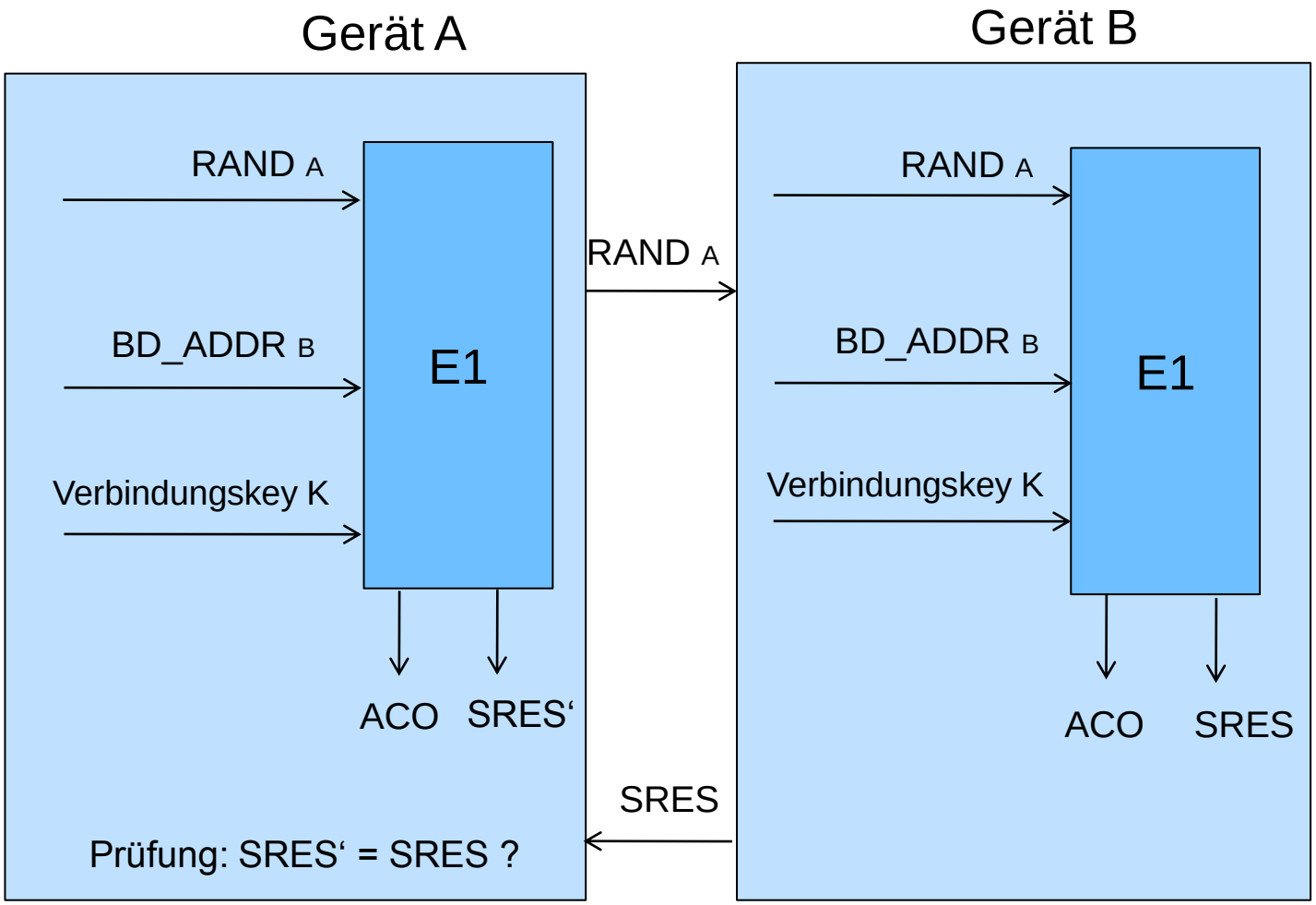


Abb. [Q1] S.876

3 Sicherheit

- Modus 1 (Non-Secure-Mode)
  - -Keine besonderen Sicherheitsmaßnahmen
  - -Frequency Hopping
- Modus 2 (Service-Level Enforced Security)
  - -Sicherheitsdienste auf Dienstebene
- Modus 3 (Link-Level Enforced Security)
  - -Absicherung auf Verbindungsebene
  - -Authentifizierung und Verschlüsselung

3.1 Sicherheitsmängel

- PIN Eingabe
- Ressourcenschwache Geräte benutzten zur Kommunikation nur die Geräteadresse

Ausblick

- Meist genutzte Technologie zur Datenübermittlung
- Neueste Version Bluetooth 3.0 – Datenübertragung mit 480 Mb/s

Abb. [Q1] S.876

Beispiel

Norwegisches Zentrum für Telemedizin

- Mithilfe der Bluetooth Wireless-Technologie wurde am Norwegischen Zentrum für Telemedizin (NST) in Tromsø eine automatisierte und drahtlose Lösung entwickelt, die die Patienten in ihrem täglichen Leben möglichst wenig beeinträchtigt.

- Die Lösung umfasst ein herkömmliches Blutzuckermessgerät, einen Bluetooth-Adapter für den seriellen Anschluss und ein Bluetooth-fähiges Mobiltelefon

[Q2]

Viel Dank für die Aufmerksamkeit !