

A stylized blue eye logo consisting of a central circle, an upper eyelid with seven rectangular rays, and a lower eyelid.

Bluetooth Security

roger.auinger@eycom.ch

Bluetooth

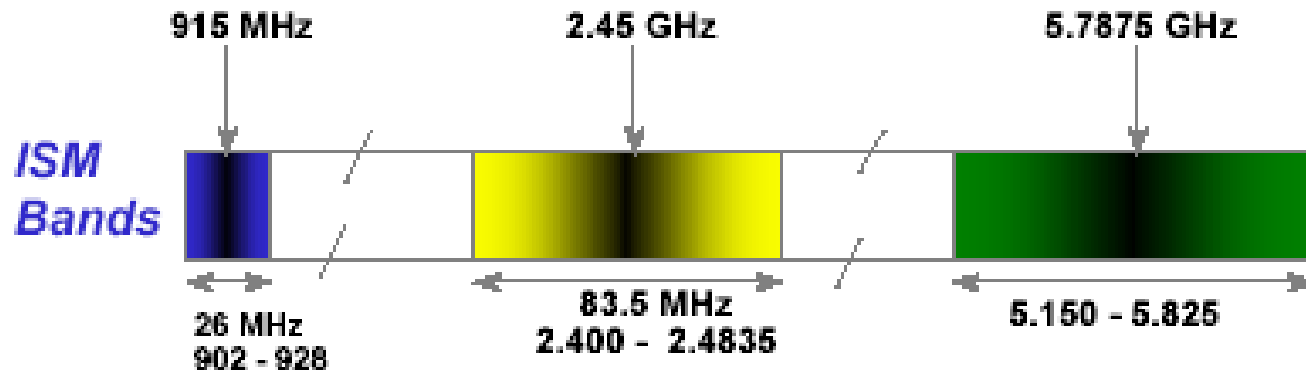
Standard für Local wireless communication

- Personal Digital Assistants (PDA's)
- Mobiltelephone
- Modems
- Laptops
- Printers

„Industry Scientific Medical“ Band

Definition:

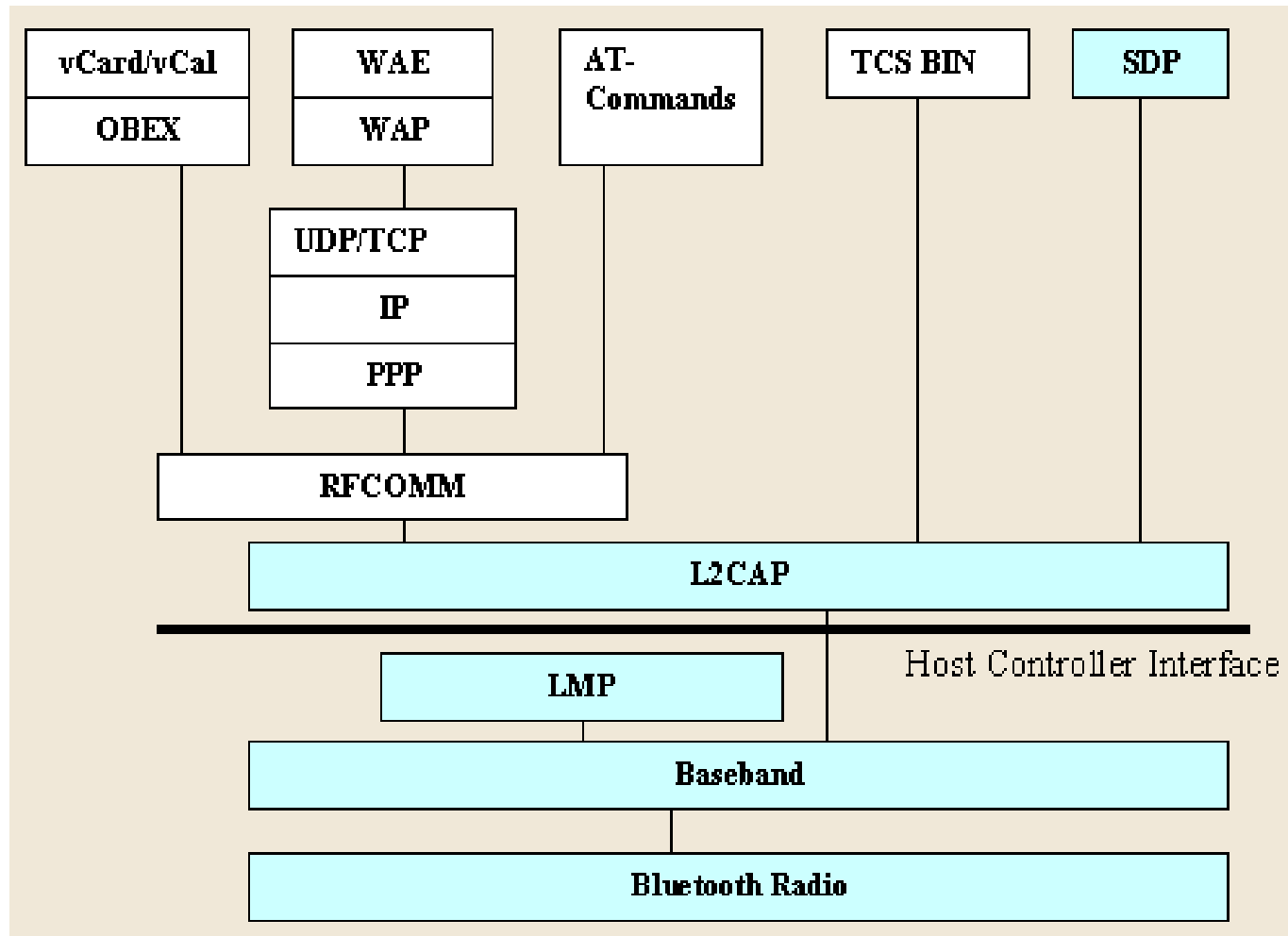
- Frequenz 2.4 bis 2.48 GHz



Spezifikation

- 2.402 – 2.480 GHz
- max. & theoretisch: 1Mb/s
- 1 asynchroner Datenkanal & bis 3 synchrone Sprachkanäle
- 1 Kanal, welcher simultan asynchron Daten und synchron Sprache übermitteln kann
- Piconets (Master/Slave-Prinzip)
- bis 10 Piconets → Scatternet

Bluetooth protocol stack



Sicherheitsprobleme

Personal Area Network (PAN)

- PAN wird mit WLAN oder LAN verbunden
- PAN ist personalisiert – Datenschutz
- Man-in-the-middle attack

Einsatz

Personal Area Network (PAN)

- z.B. PDA mit PC um eMails zu schreiben
- z.B. Mobiltelephone als Modem mit PDA

Public

- z.B. Airport: Download Flugplan

Authentisierung von Geräten nicht von Personen

Sicherheitsoptionen I

Security mode 1:

Promiscuous oder Discovery mode

Security mode 2:

Sicherheit nach Verbindungsaufbau

Security mode 3:

Chiffrierung und Authentisierung vor Verbindungsaufbau

Sicherheitsoptionen II

- Bluetoothadresse (48 bit)
 - Unique, definiert durch IEEE
- Authentisierungskey (128 bit)
 - Zufallszahl (random number)
- Chiffrierungskey (8-128 bit)
- Zufallszahl (128 bit)

Initialisierungskey

- Dient zum Key-exchange
- Chiffrierung: $f(\text{PIN}, \text{Länge PIN}, \text{Zufallszahl})$
- PIN ist default = 0000

Chiffrierung

- Stream ciphering
- Algorithmus E_0 :
 - Input: Zufallszahl, Bluetoothadresse Master, Clock Master, Chiffrierkey
 - Output: cipher stream

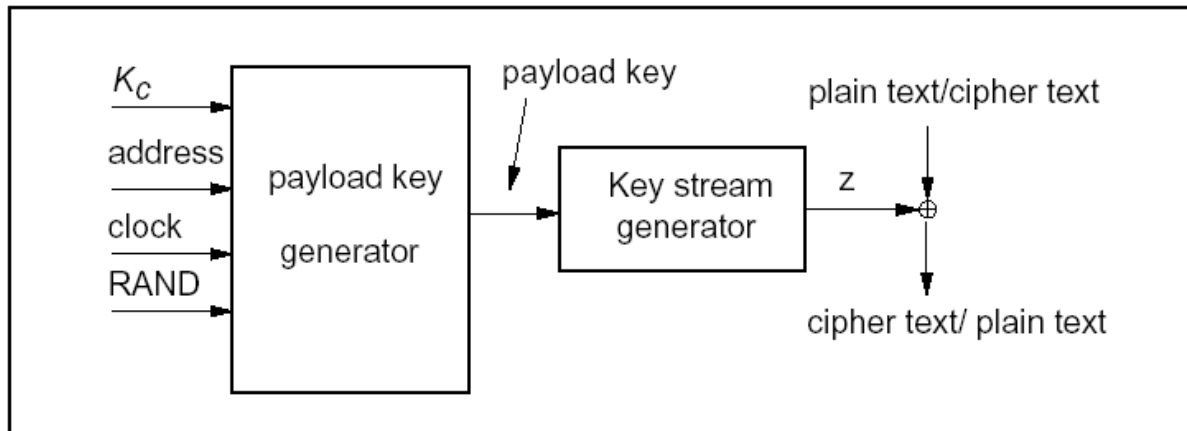


Figure 14.4: Stream ciphering for Bluetooth with E_0 .

Unterschiede zwischen den Standards: Bluetooth und IEEE 802.11b?

- ❖ IEEE 802.11b ist eine zur verkabelten Welt (Ethernet) ergänzende Technologie → Wireless LAN (grosse Datenmengen, n Benutzer) Bluetooth ist eine kabellose Technologie zur Kommunikation zwischen verschiedenen mobilen Geräten („Wireless USB“) → Wireless PAN (kleine Datenmengen, meistens 1 Benutzer)

Ist der Einsatz von Bluetooth-Produkten sicher?

- ❖ Bedingt. Unter gewissen Umständen ist das Knacken des Initkeys und somit des Chiffrierkeys möglich. End-to-End Sicherheitsprinzip wird nicht unterstützt. Risiken: Authentisierung (Gerät authentisiert und nicht Benutzer), Key-distribution, „Location Attack“

Auswahl an Produkten



Foto: Ericsson



Links

www.bluetooth.com

www.sans.org

www.niksula.cs.hut.fi/~jiitv/bluesec.html

www.inf.ethz.ch/vs/edu/SS2001/MC/beitraege/08-security-rep.pdf

grouper.ieee.org/groups/802/11/index.html