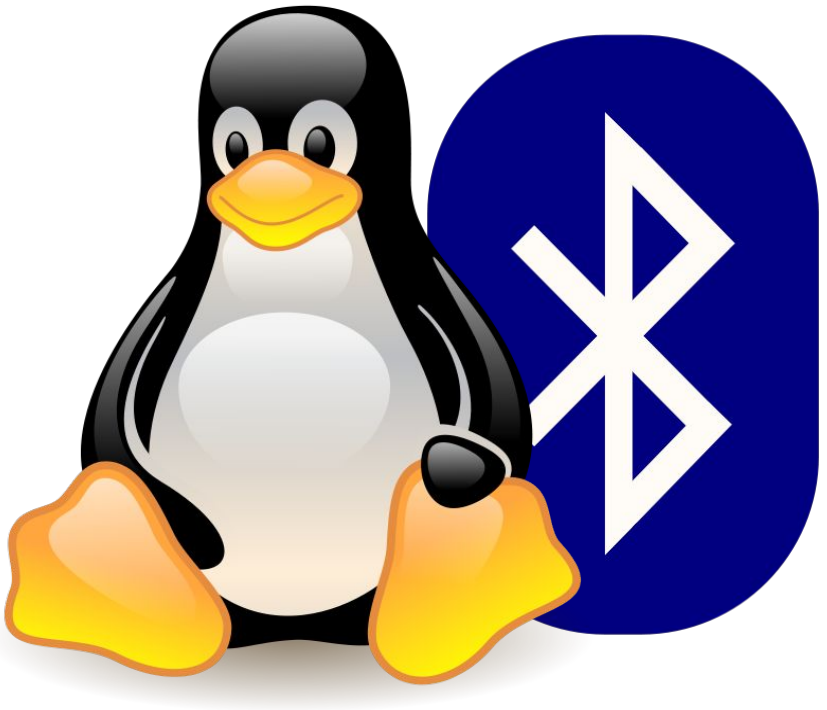
Bluetooth unter Linux



Steffen Bauer, Vortrag 24/04/2012 Linux User Group Frankfurt am Main

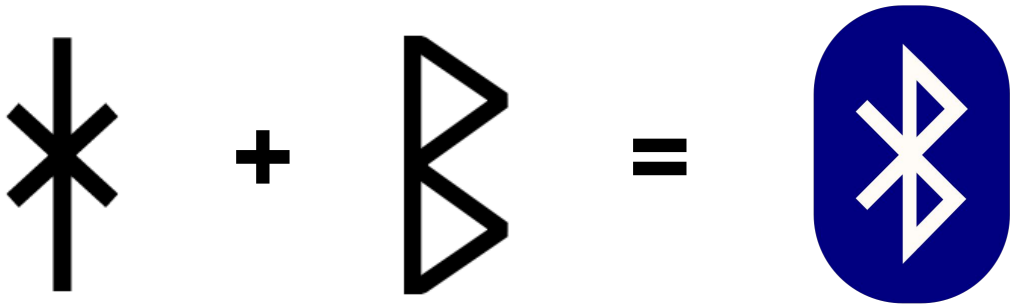
Historie Bluetooth

- 80er: Erste Versuche mit schnurlosen Eingabegeräten (1983 erste IR-Maus, Logitech, für *Metaphor Computer*)
- 1993 Gründung der *Infrared Data Association* (IrDA)
- 1994 Ericsson beginnt mit Forschung zum funkbasierten Ersatz (Nachteil Infrarot: Sichtverbindung notwendig)
- 1998 Gründung der *Bluetooth Special Interest Group*
- 2001 Standard Version 1.1, erste solide Basis für marktfähige Produkte

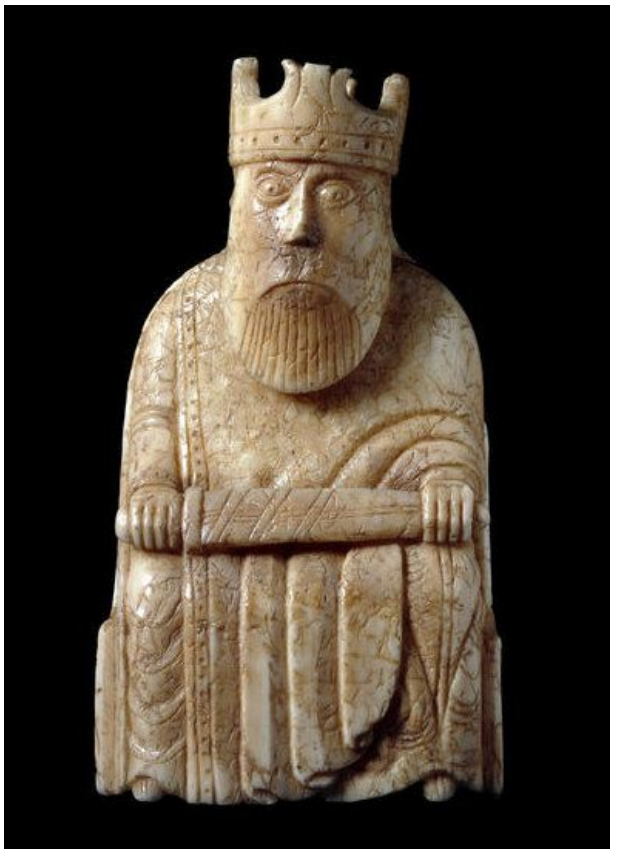
Metaphor Computer Systems, 1983

Historie: Namensgeber Harald I 'Blåtand' Gormsson ('Blauzahn')

- Namenswahl durch skandinavische Mitglieder der Bluetooth Special Interest Group
- König Dänemarks von ca. 958 - 970
- Kurioser Ehrenname „Blauzahn“ evtl. Fehltranskription
- Galt als fähiger Diplomat und Kommunikator, vereinigte die verfeindeten Stämme Skandinaviens
- Bluetooth-Symbol aus den Initialen Haralds in altnordischer Runenschrift:



Hagall + **B**jarkan = **Bluetooth**



König aus den Schachfiguren von Lewis, 12. Jht, Norwegen

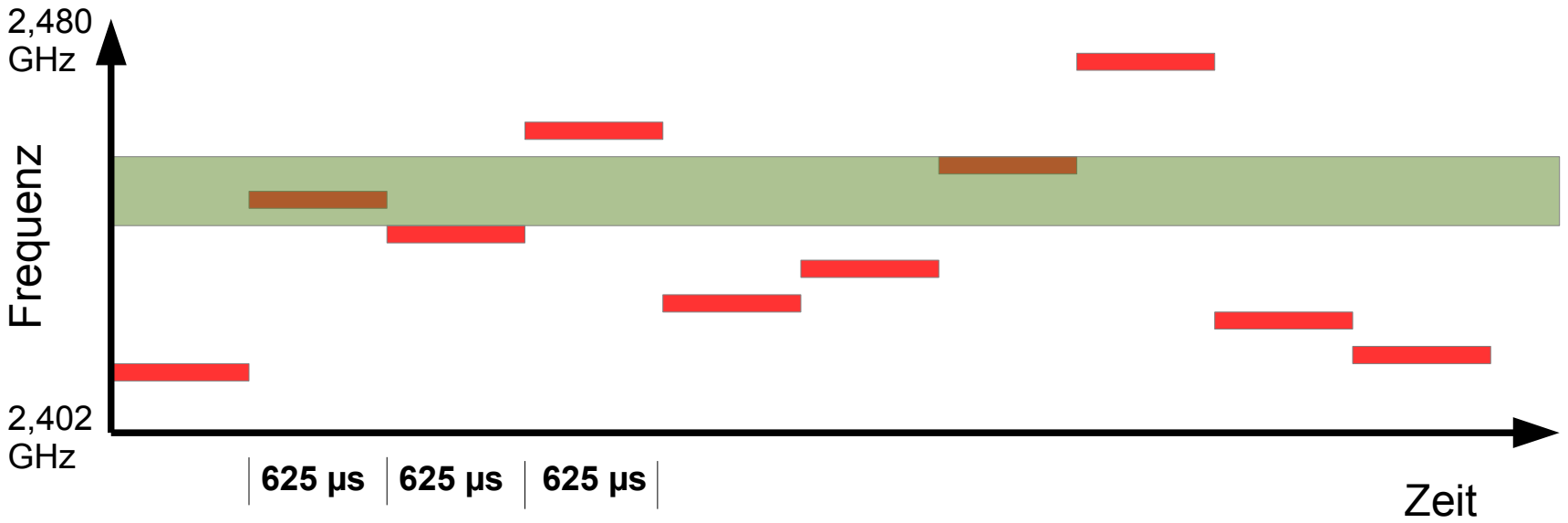
Bluetooth vs. WLAN

	Bluetooth	WLAN
Funkfrequenz	2,4 GHz	2,4 / 5 GHz
Reichweite	< 10m bis < 100 m	< 100m
Strahlungsleistung	Niedrig (2,5 mW bis 100 mW)	Mittel (100+ mW)
Datenrate	768 kbps - 2 Mbps	1 Mbps - 54 Mbps
Einsatz	Kommunikation mit Kleingeräten	Netzwerk

Bluetooth Versionen

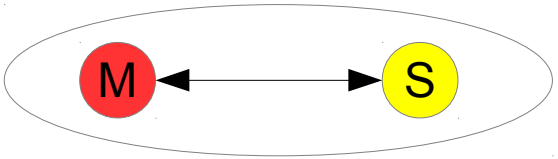
Version	Features	max. Datenrate
V1.0 / V1.0B	Etliche Sicherheitsprobleme; aufgegeben	732 kbit/s
V1.1	Erste marktreife Version	732 kbit/s
V1.2	Adaptive Frequency Hopping	1 MBit/s
V2.0 + EDR	Enhanced Data Rate	2.1 MBit/s
V2.1 + EDR	Erweiterte Sicherheitsfeatures (Secure Simple Pairing)	2.1 MBit/s
V3.0 + HS	Zusätzlicher High Speed Kanal	24 MBit/s (über separaten Kanal)
V4.0	Low Energy Mode	24 MBit/s (HS) 1 MBit/s (Low Energy)

Technik: Frequenzhopping

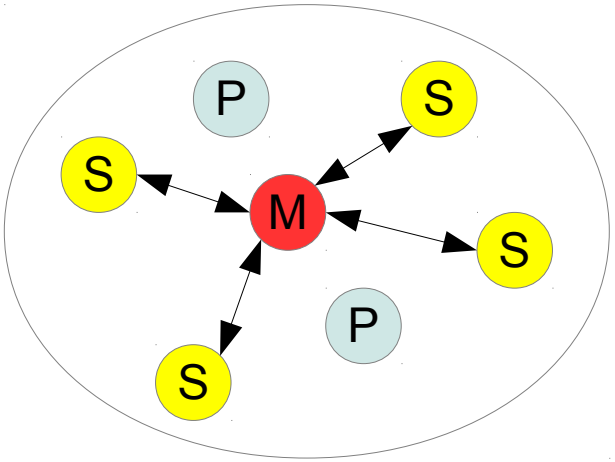


- Bluetooth arbeitet im freien ISM-Band (**I**ndustrial-**S**cientific-**M**edical)
- Reduzierung von Störungen durch Frequenzsprungverfahren (WLAN, Mikrowelle usw. arbeiten im gleichen Frequenzband)
- Hoppingsequenz ist pseudozufällig, wiederholt sich alle knapp 24 Stunden
- Verbundene Bluetoothgeräte müssen sich synchronisieren

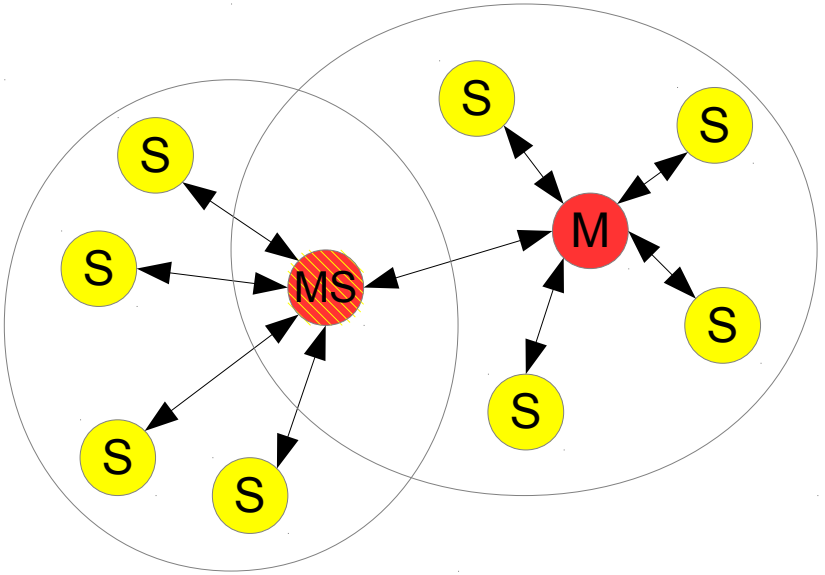
Bluetooth Netzwerktopologien



1) **Point-to-Point** (Master/Slave)



2) **Piconet** (1 Master, 7 Slaves, 254 Parked)



3) **Scatternet** (bis zu 10 Piconets, selten)

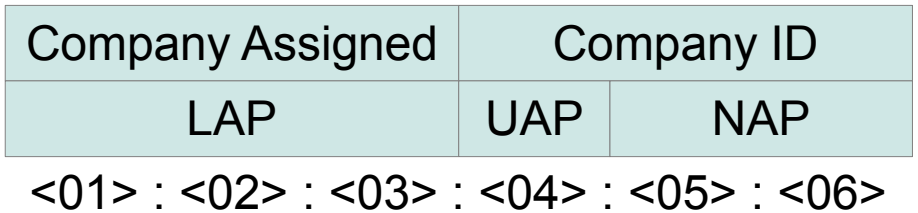
Bluetooth Basics

- Bluetooth Datenpaket

- Bluetooth Pakettypen

ACL	SCO
Asynchronous ConnectionLess	Synchronous Connection Oriented
Packet retransmission	No retransmission
Asymmetrisch	Bidirektional
Alle sonstigen Daten	Sprache / Telefonie

- Bluetooth Adresse (MAC-48, little endian)



Bluetooth Basics

Bluetooth Protokolle:

- L2CAP — Basisverwaltung von Bluetooth Verbindungen
- SDP — Service Discovery Protocol
- HIDP — Human Interface Device Protocol
- AVDTP — Audio Video Distribution Protocol
- SCO — Synchrone Audioverbindungen
- RFCOMM — Emulation Serielle Schnittstelle
- BNEP — Emulation Ethernet
- (OBEX) — Object Exchange (kein originäres Bluetooth Protokoll)

Bluetooth Profiles:

- DUN/PAN — Netzwerkverbindung
- HSP — Headset Mono Audio
- A2DP — Stereo High Quality Audio
- HID — Human Interface Device
- SPP — Serial Port Profile
- OPP — Object Push Profile
- FTP — File Transfer Profile
- SP — Synchronization Profile
- HDP — Health Device Profile
- ... — ... und noch viele andere

Bluetooth stack

Datei manager

Network

X evdev

Bluetooth manager

Audio

Headset

OBEX

DUN

PAN

HID

SDAP

A2DP

RFCOMM

BNEP

HIDP

SDP

AVDTP

SCO

L2CAP

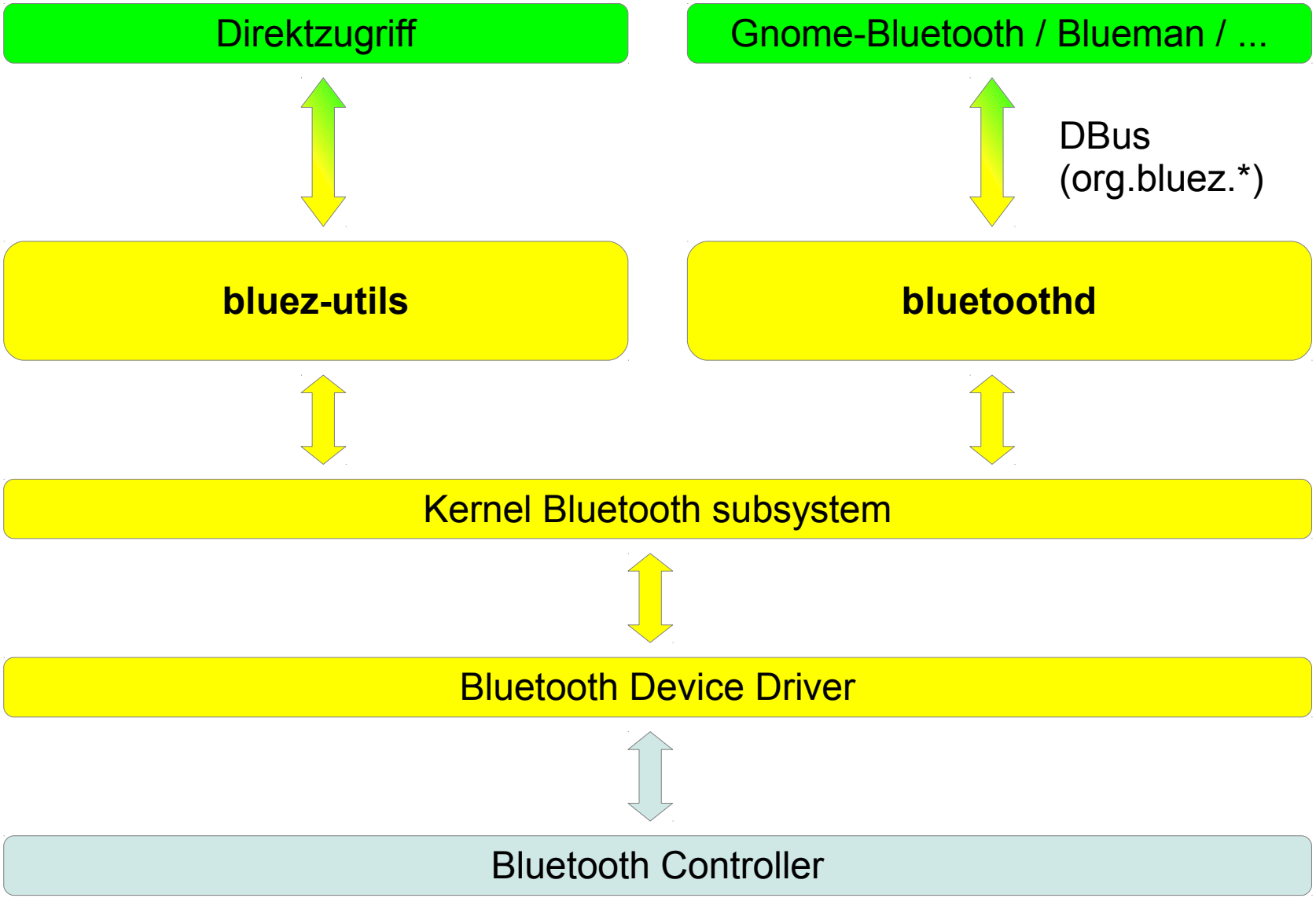
Host controller interface HCI

Link Management Protocol

Baseband Link Controller

Bluetooth Radio

Bluetooth Linux Integration (bluez)



Bluetooth Sicherheit: Basics

- **Discoverability**
  - Meist manuell de/aktivierbar
  - Legt fest ob Gerät auf eine *Device Discovery* Anfrage reagiert
  - Aber: Bluetoothgeräte reagieren **immer** auf L2CAP / SDP Anfragen per direkter Bluetooth-Adresse!

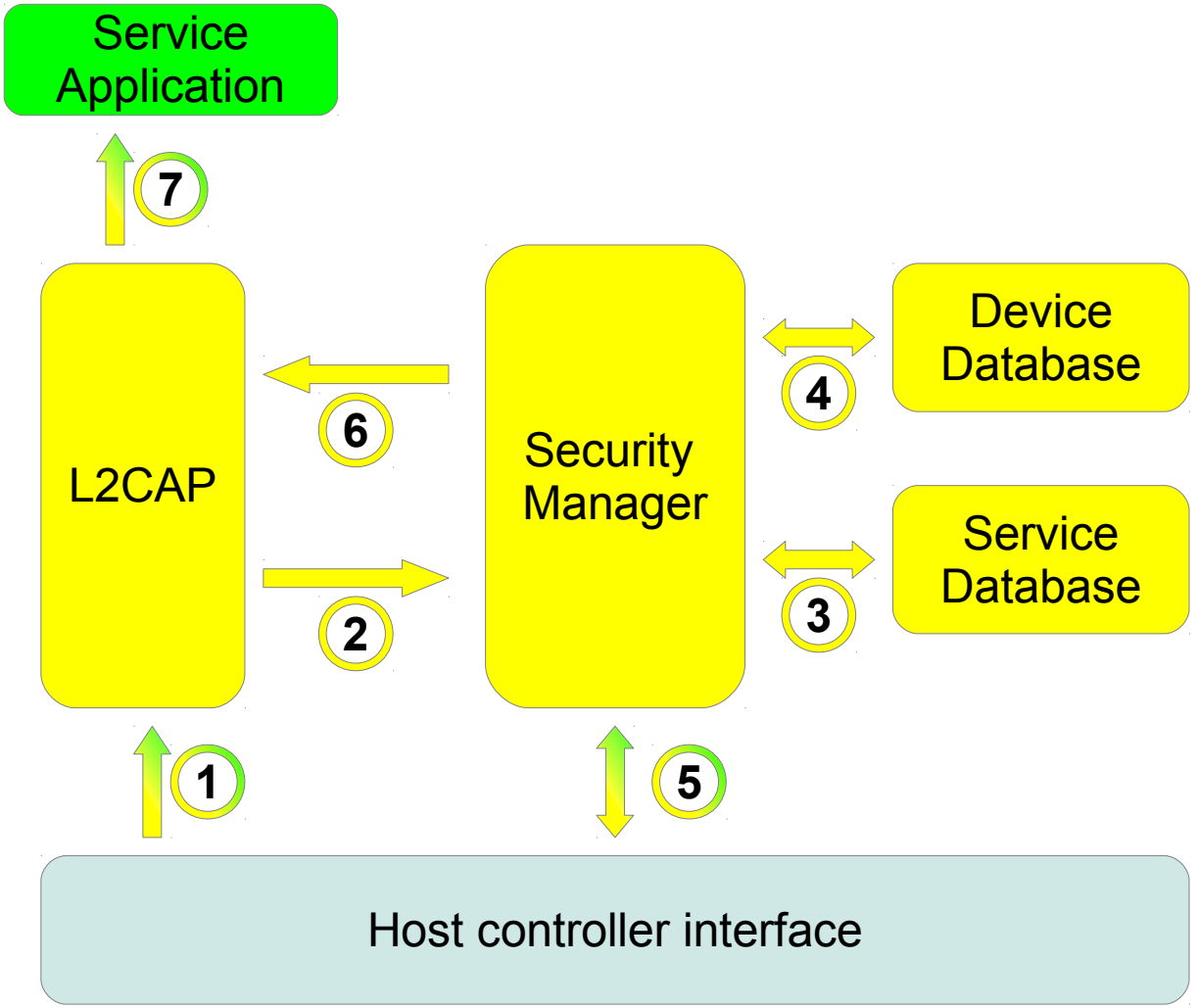
- **Service security levels**, regelt Zugriff auf einzelne Bluetooth-Dienste:

  1) Offen für **alle** anfragenden Geräte (SDP, häufig OPP)
  2) Nur **authentifizierte** Geräte
  3) Nur **authorisierte** Geräte (FTP, DUN etc.) ('trusted', impliziert Authentifizierung)

- **Pairing**
  - Vorgang um Geräte gegenseitig zu authentifizieren
  - Austausch von Link Keys generiert aus Initial-PIN und Zufallsseed
  - Achtung: Gepairtes Gerät wird häufig automatisch als 'trusted' gekennzeichnet!
  - Link Key wird in Datenbank abgelegt für zukünftigen Zugriff
  - Zwei Geräte mit fester PIN können nicht gepairt werden

Bluetooth Sicherheit: Authorization

1. Anfrage von externem Gerät
2. L2CAP Anfrage an Security Manager
3. Security Manager prüft ob angeforderter Service Authorisation braucht
4. Falls ja, Prüfung ob Gerät bereits authentifiziert / authorisiert
5. Evtl. Durchführung von Neuauthentifizierung
6. Rückmeldung an L2CAP
7. L2CAP gibt Service je nach Ergebnis frei / sperrt



Bluetooth Sicherheit: Angriffsmöglichkeiten

(Mostly) Social Engineering Angriffe

- *Bluejacking*: Senden unerwünschter Nachrichten über offenes OBEX Push
- *Car Whispering:* Einschleusen von Audio in Headsets über Standard-PIN
- *Authentication abuse:* Zugriff auf Systemdienste nach erschlichenem Pairing
- Discoverable Mode verrät Anwesenheit und Name eines (teuren) Smartphones / Laptops (Real Life: Serie von Autoaufbrüchen in Cambridgeshire)

Denial of Service Angriffe

- *BlueSmack:* DOS Angriff mittels L2CAP echo request flood
- *BlueStab:* „Ping of death“-Lücke in div. Smartphones (Control chars führen zu Crash)
- *BlueChop:* Deauthentication Angriff auf Pico-/Scatternets

Exploits (meist Firmwarebugs in älteren Handys)

- *BlueSnarf:* OBEX Pull von bekannten Objekten (z.B. Adressbuchdatei)
- *BlueBug:* Einschleusen von AT-Kommandos (Anwahl von 0900-Nummern)
- *HeloMoto:* Fortgeschrittener Snarf-Angriff, Angriffsgerät bleibt nach bewusstem Pairingabbruch als Trusted Device im Cache
- *BTCrack:* Abhören des Pairing-Vorganges / Übernahme der Verbindung

Bluetooth Sicherheit: Countermeasures

- Vorteil von Bluetooth: Kurze Reichweite (z.B. bei DOS-Angriff: Weglaufen)
- Frequenzhopping erschwert passives Scannen
- Echte Hardware-Bluetoothsniffer sind nicht leicht verfügbar

- Bei Menschenansammlungen vorsichtig sein (Flughäfen, Kongresse etc.)
- Am besten: Bluetooth nur aktivieren, wenn es gebraucht wird
- Nur unbedingt benötigte Dienste freigeben
- Fremde Geräte nicht ohne weiteres als „trusted“ kennzeichnen
- 'Discoverable Mode' nur zum Pairing aktivieren
- Pairing in sicherer Umgebung durchführen
- Wenn Verbindung nicht mehr benötigt wird, Gerät aus Liste löschen
- Ebenso bei Diebstahl Gerät aus Liste löschen
- Bei unerwarteten Anfragen nicht automatisch 'Akzeptieren' klicken!