

Aufbau eines Sensornetzes mit LoRaWAN

Funk für Bereiche, die sich mit WLAN nicht abdecken lassen

Chris Fiege – c.fiege@pengutronix.de



Wer bin ich?

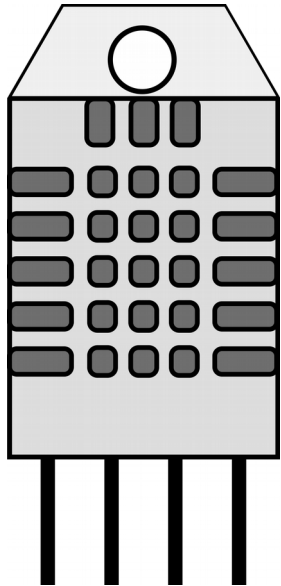
- Chris Fiege
- Hardware Entwickler

- Einarbeitungsprojekt:
Software

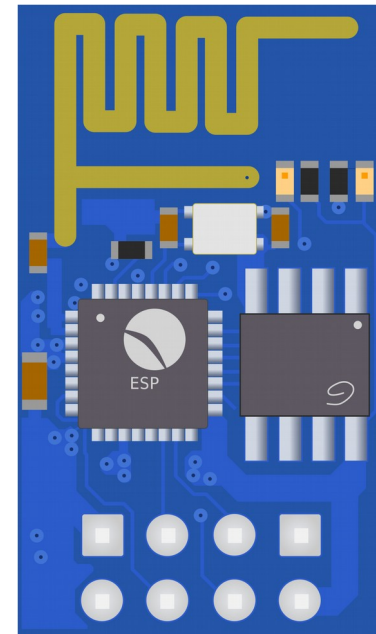


Home Automation: WLAN

WLAN für Microcontroller



CC0 1.0 adlerweb@opencipart.org



CC0 1.0 adlerweb@opencipart.org



Erfassung von Feinstaubwerten über das eigene WLAN



Größere Reichweiten?

- Anwohner überreden: WLAN-Zugang
- Mobilfunk
 - M2M-Zugang monatlich:
2€ für 5MB
3€ für 50MB
 - 1nce.com:
10€ für 500MB in 10 Jahren



LoRaWAN



LongRange Wide Area Network



LoRaWAN

- Industriestandard
- LoRa Alliance

- Geschlossener Standard
- admin@mail.lora-alliance.org
„Please send specification and regional parameters“



LoRaWAN: Fakten

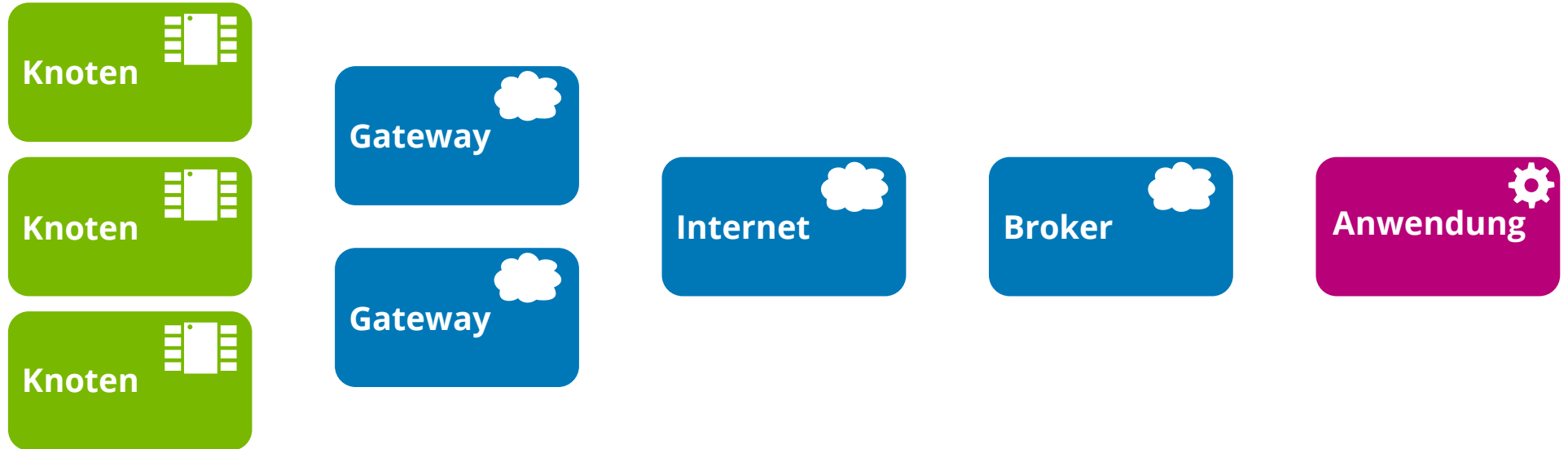
Thema	Fakt
Bänder:	EU: ISM Bänder: 433 MHz und 868 MHz
Sendeleistung:	25 mW (14 dBm)
Modulation:	Spread Spectrum (Chirped FM)
Datenrate	0.3 .. 50 kBit/s
Reichweite:	2 km .. 10 km
Nachrichtenlänge:	51 .. 222 Bytes
Verschlüsselung:	AES ECB (128 Bit Schlüssel)



LoRaWAN



Netzwerkaufbau



Infrastruktur

Kommerziell

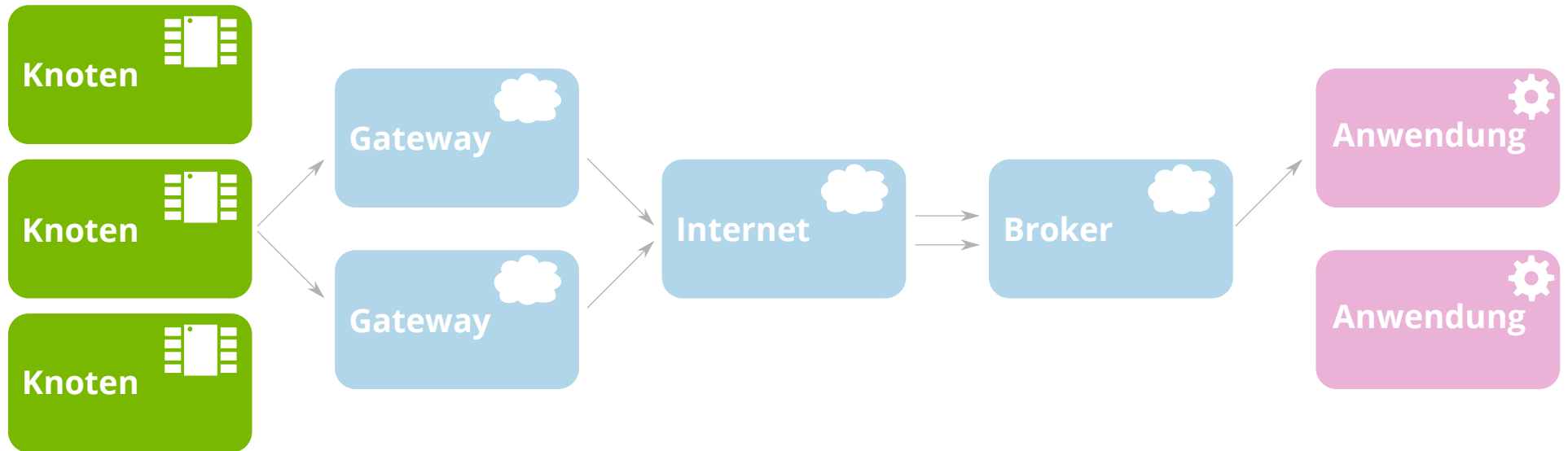
- z.B. Mobilfunkbetreiber
- Gateways
- Broker

Community

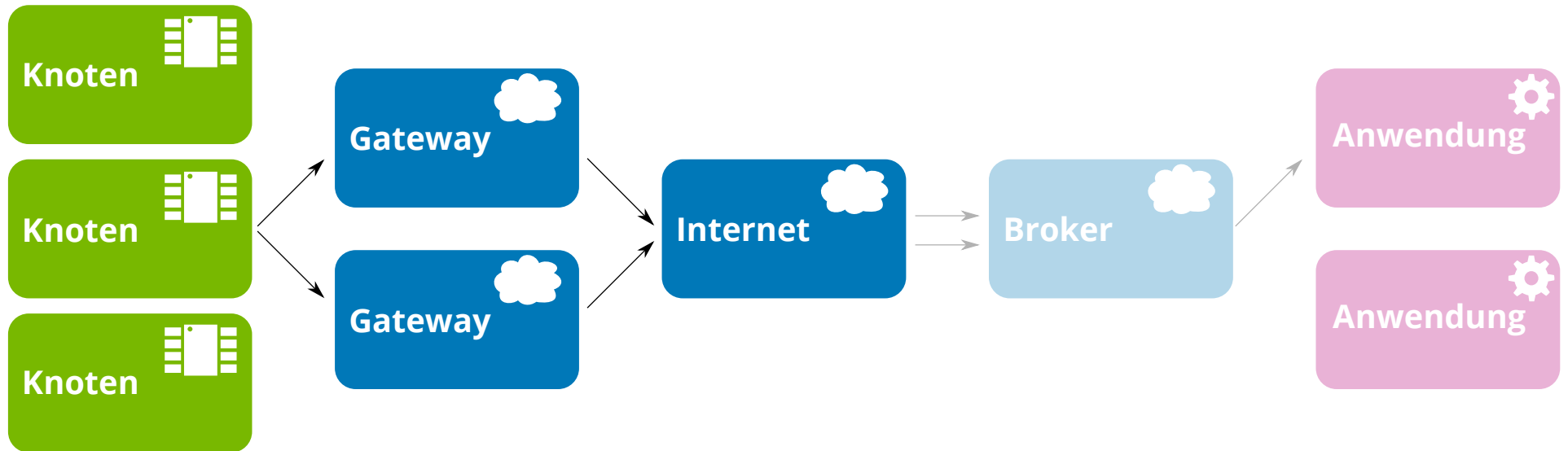
- z.B. TheThingsNetwork.org
- Broker
- Anwendung



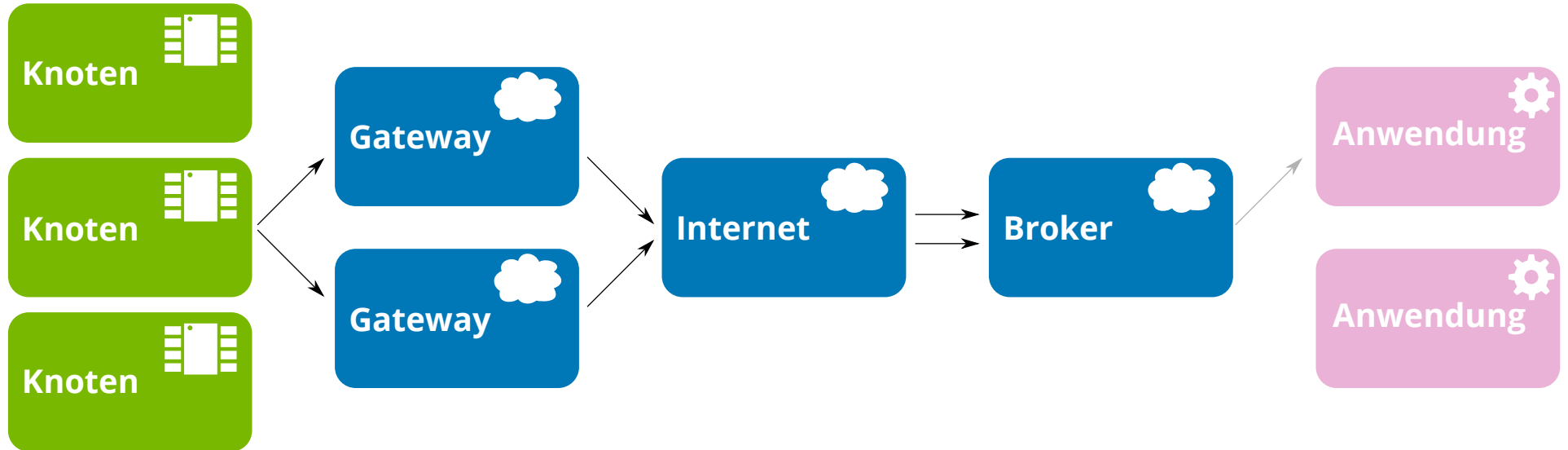
Netzwerkaufbau: Uplink



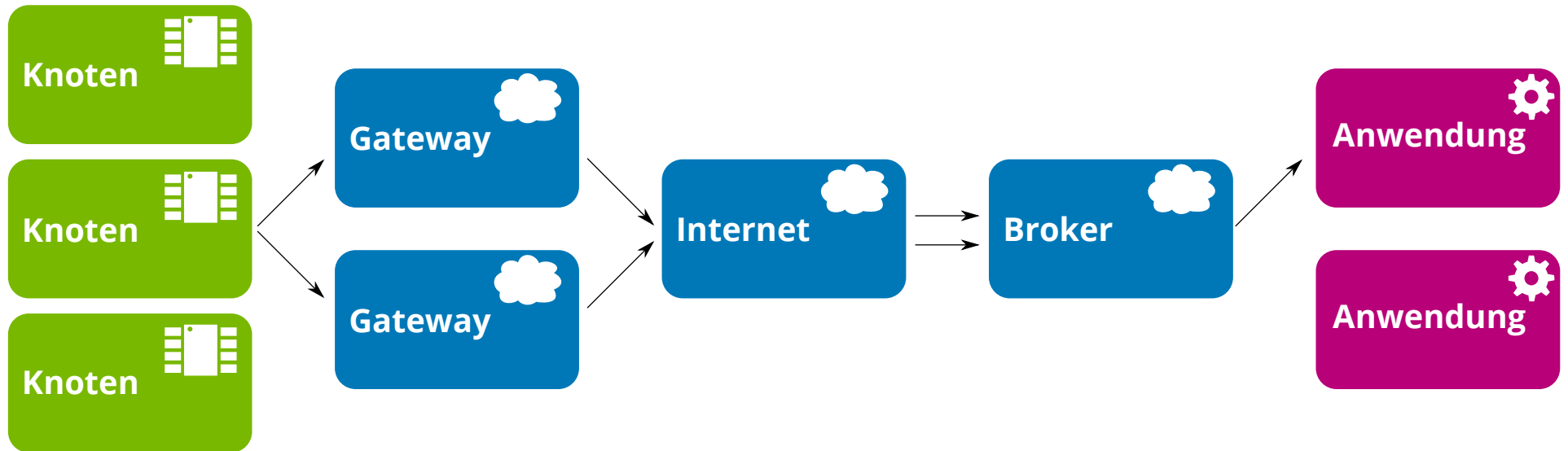
Netzwerkaufbau: Uplink



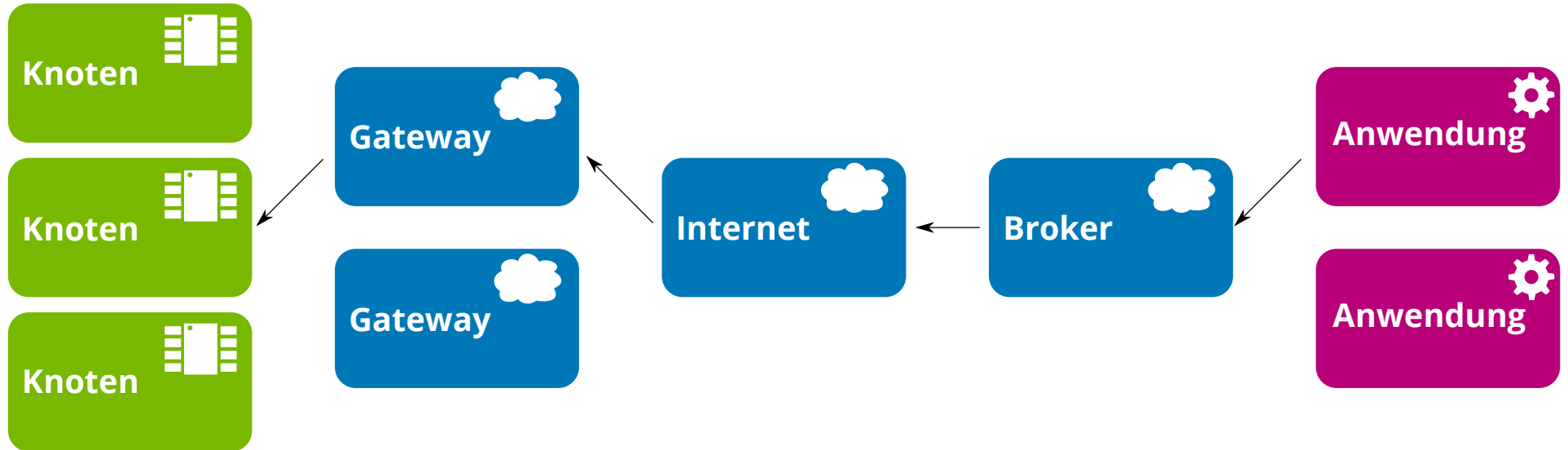
Netzwerkaufbau: Uplink



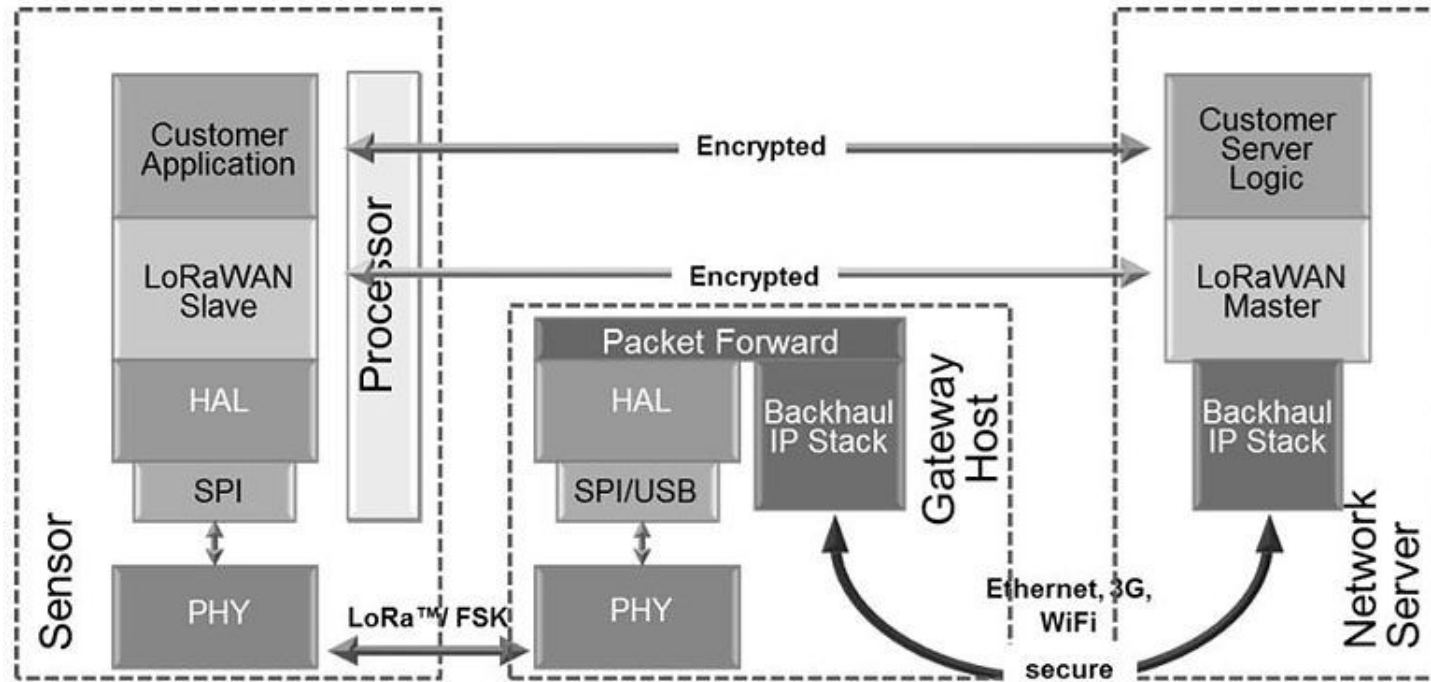
Netzwerkaufbau: Uplink



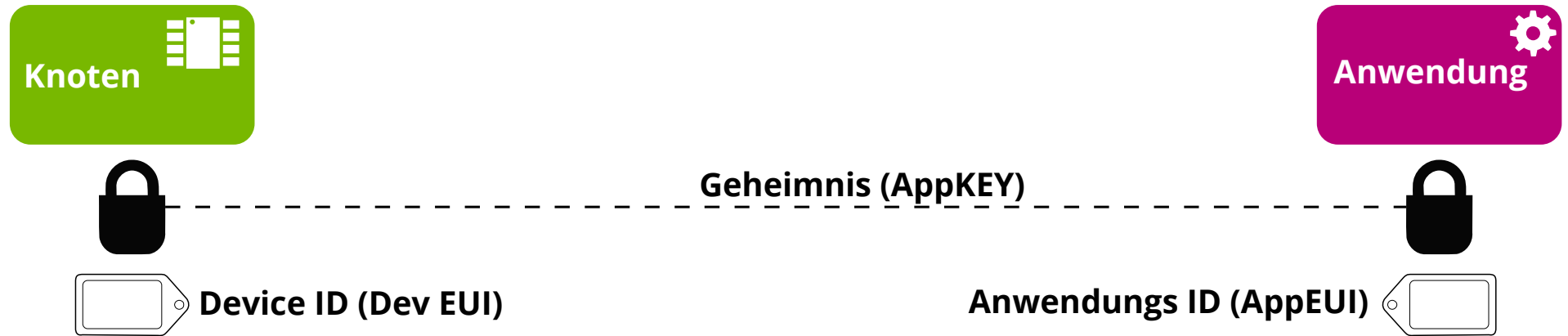
Netzwerkaufbau: Downlink



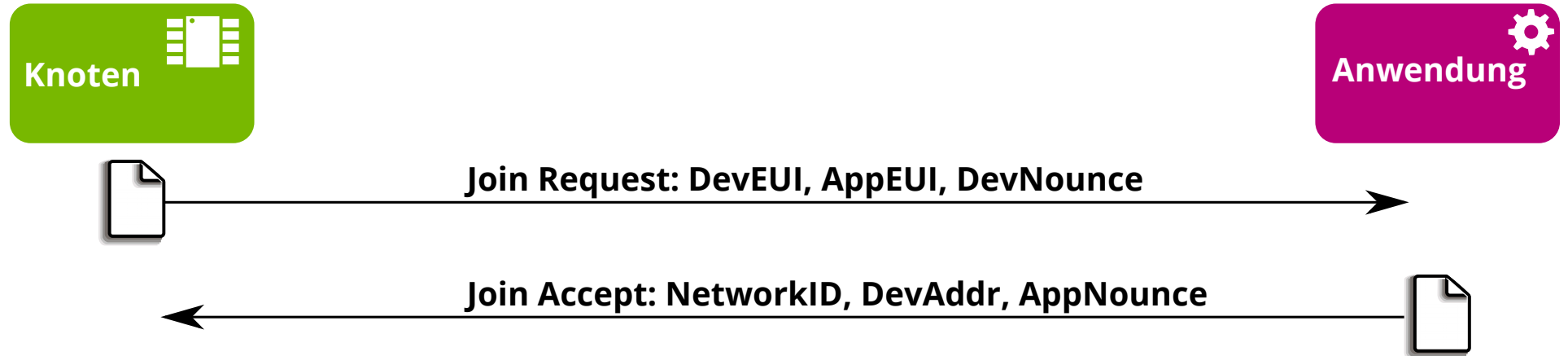
Netzwerkaufbau



Verschlüsselung: Geteiltes Geheimnis



Verschlüsselung: Sitzungsschlüssel



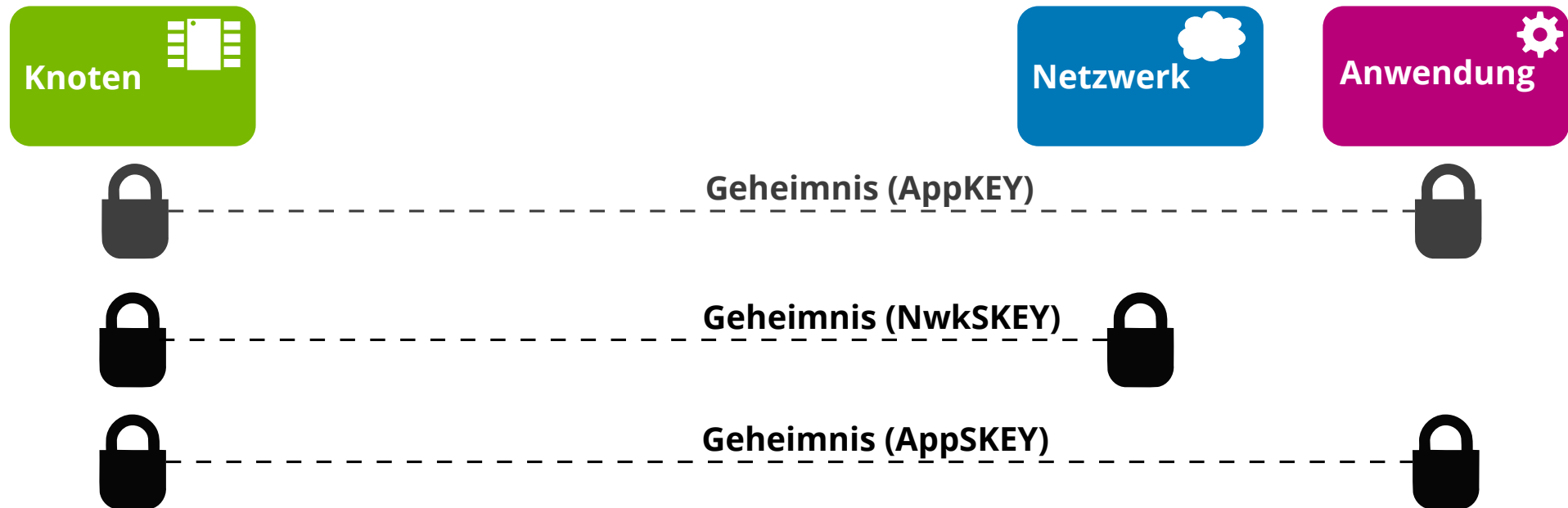
Verschlüsselung: Sitzungsschlüssel

```
NwkSKey: aes128_encrypt (AppKey,  
                          AppNounce |  
                          DevNounce |  
                          NetID |  
                          0x01 [| Padding] )
```

```
AppSKey: aes128_encrypt (AppKey,  
                          AppNounce |  
                          DevNounce |  
                          NetID |  
                          0x02 [| Padding] )
```

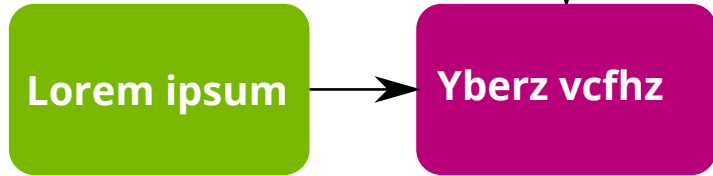


Verschlüsselung: Sitzungsschlüssel

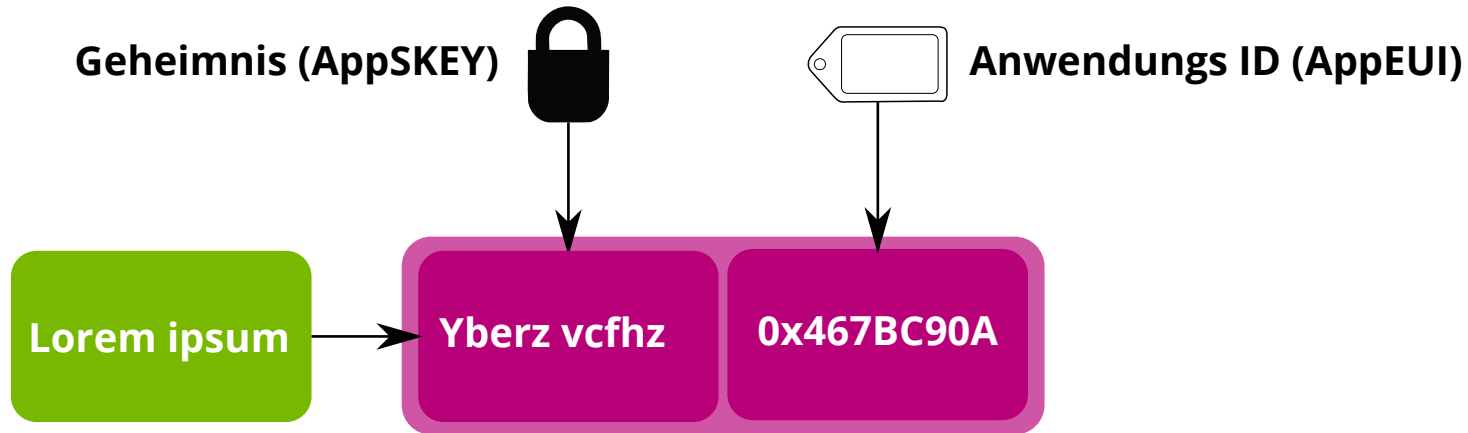


Verschlüsselung

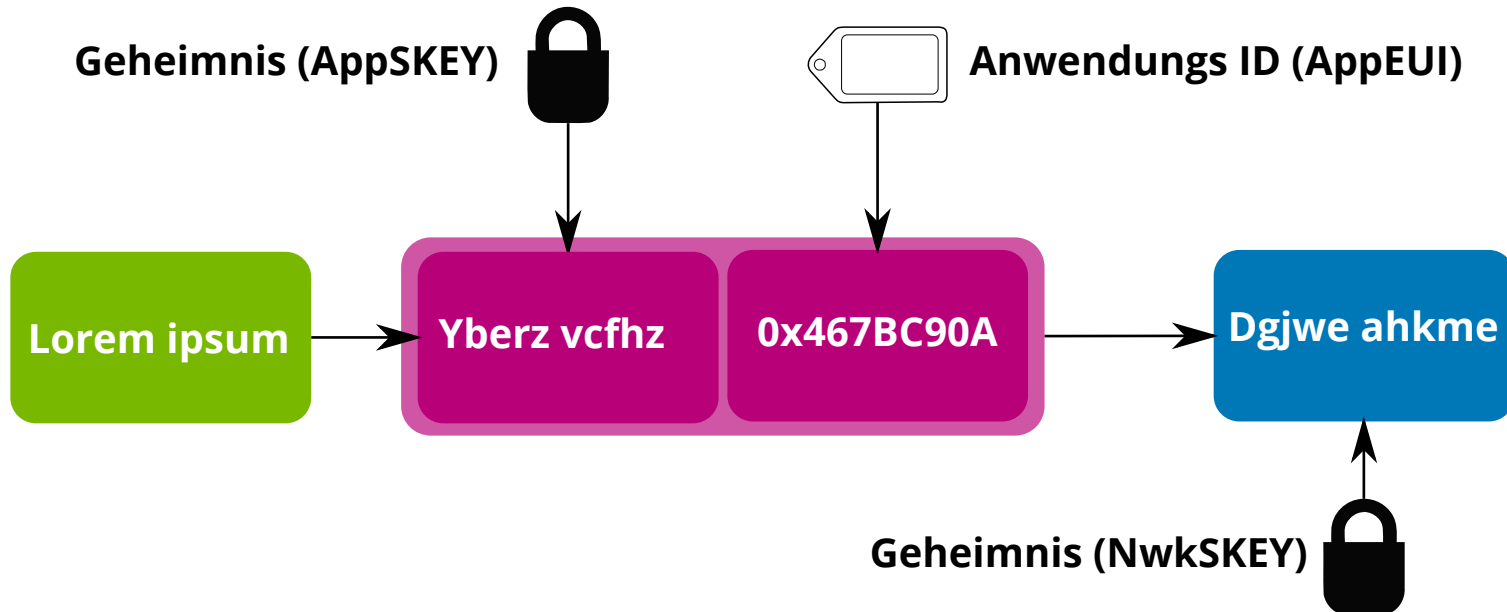
Geheimnis (AppSKEY) 



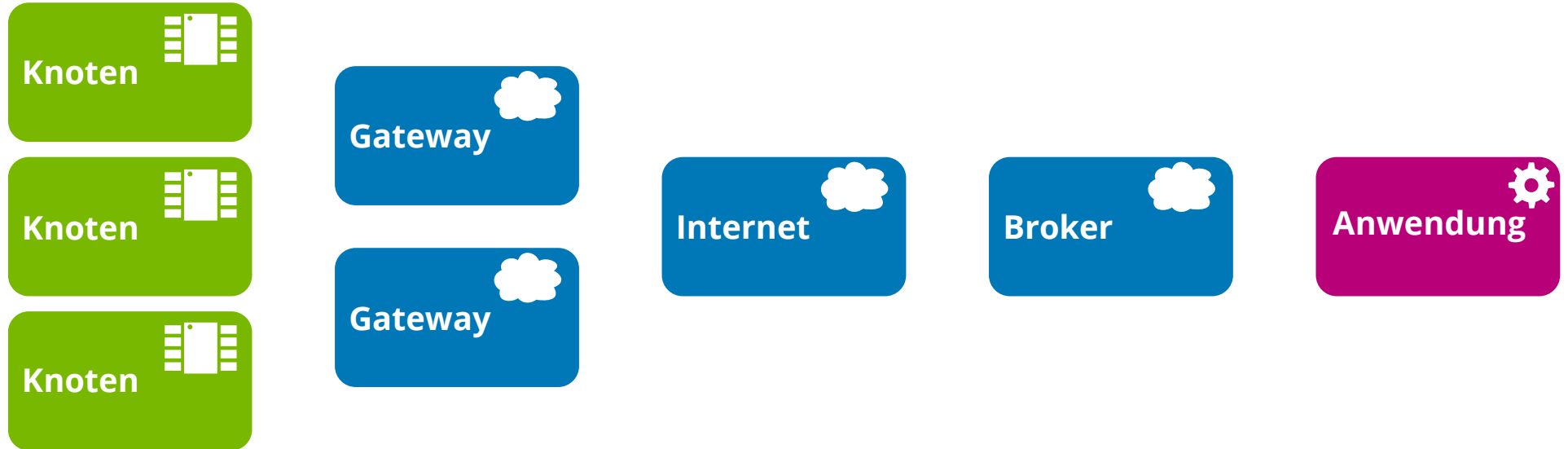
Verschlüsselung



Verschlüsselung



Netzwerkaufbau



Verschlüsselung: Leftovers

- Device: Immer aes_encrypt
App: Immer aes_decrypt
- Prejoined Nodes:
 - *Session*-Keys für die Lebensdauer des Knotens



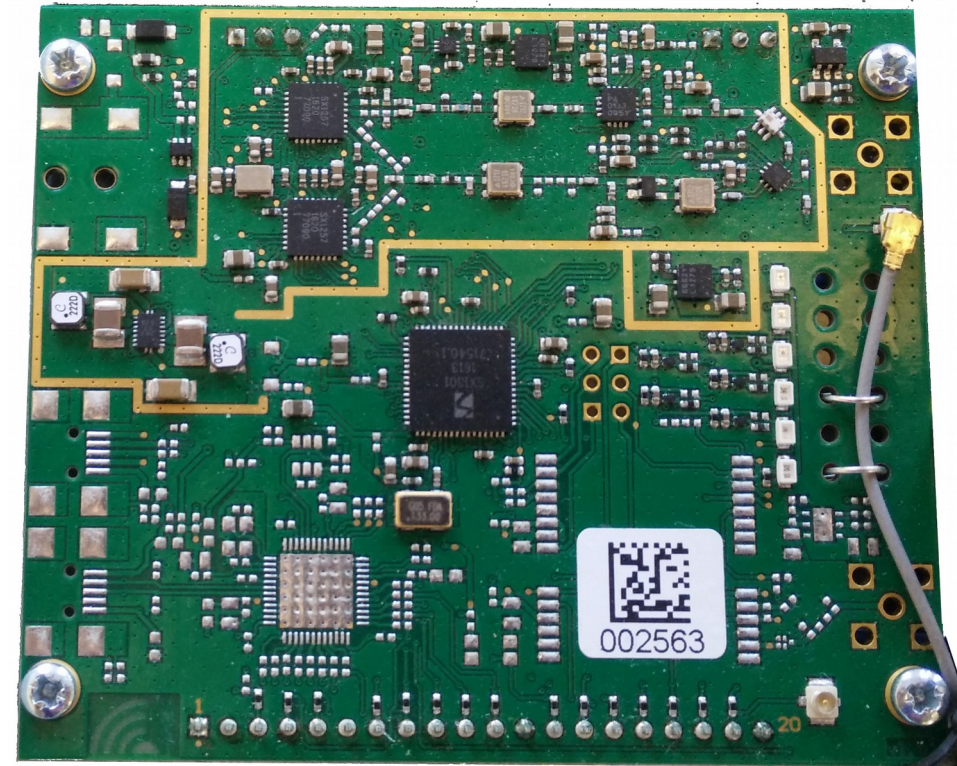
Gateway im Eigenbau: Hardware



Gateway im Eigenbau: Hardware

IMST iC880A

- 8 Pakete gleichzeitig empfangen
- 2 gleichzeitig senden
- 868MHz
- SPI-Interface
- ca. 150€



Gateway im Eigenbau: Hardware

Beagle Bone Black: 40€

Antenne: 20€

Gehäuse: 30€



Gateway im Eigenbau: Software

Referenzimplementierung zum iC880A:

- libloragw:
https://github.com/Lora-net/lora_gateway
- Packet Forwarder:
https://github.com/Lora-net/packet_forwarder



Gateway im Eigenbau: Software



Integration in Distrokit:

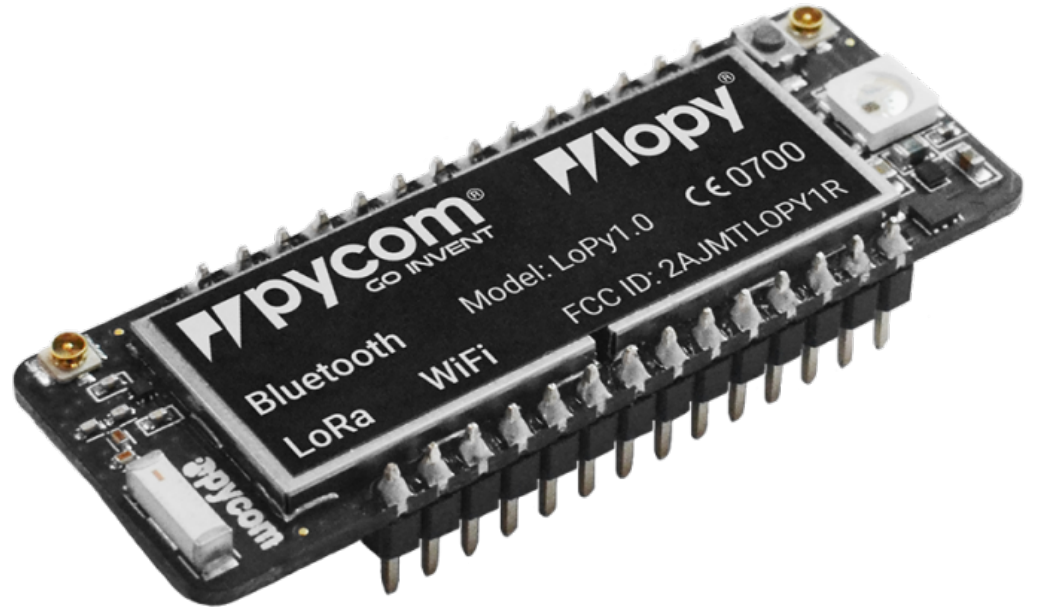
<https://git.pengutronix.de/cgit/DistroKit/>



Knoten im Eigenbau: Hardware

pycom LoPy

- WLAN, Bluetooth, LoRa
- ca. 40€



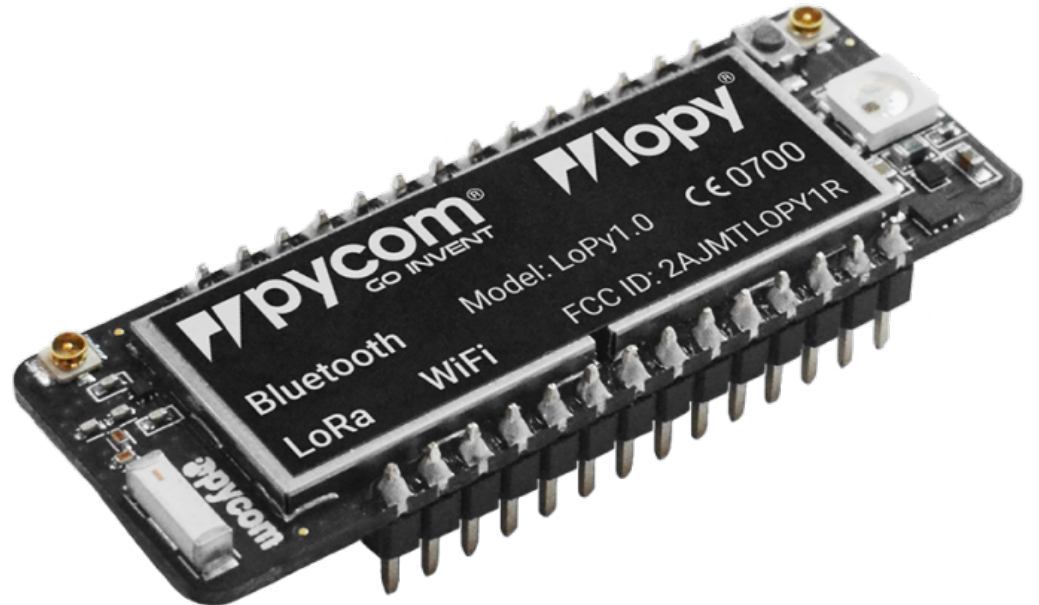
<https://pycom.io>



Knoten im Eigenbau: Hardware

Nicht gelöste Fragen:

- Gehäuse
- Energiespeicher
- Energieerzeugung
- Debugging im Feld



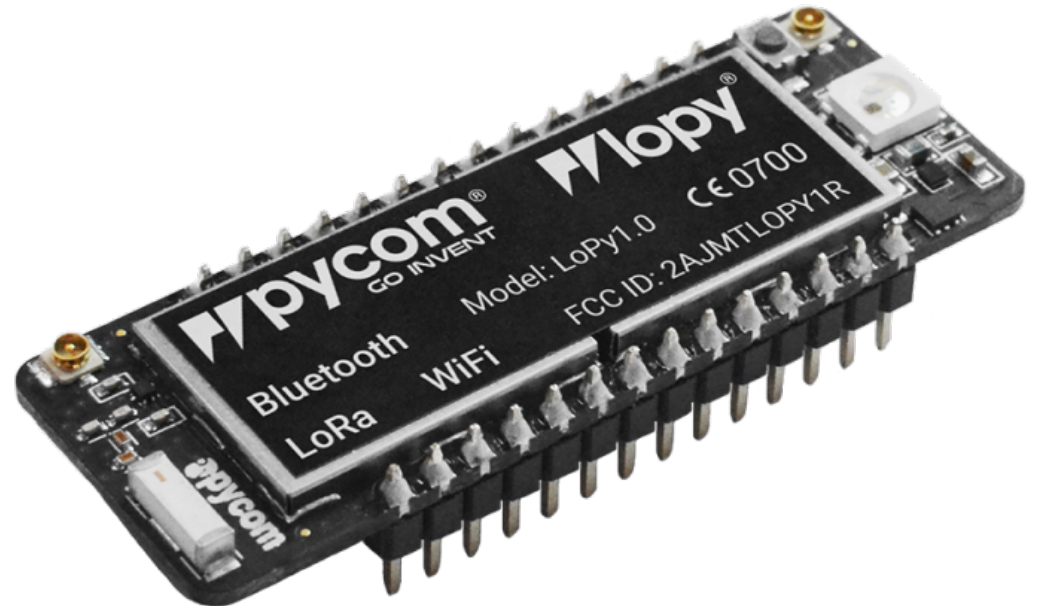
<https://pycom.io>



Knoten im Eigenbau: Hardware

Gelöste Fragen:

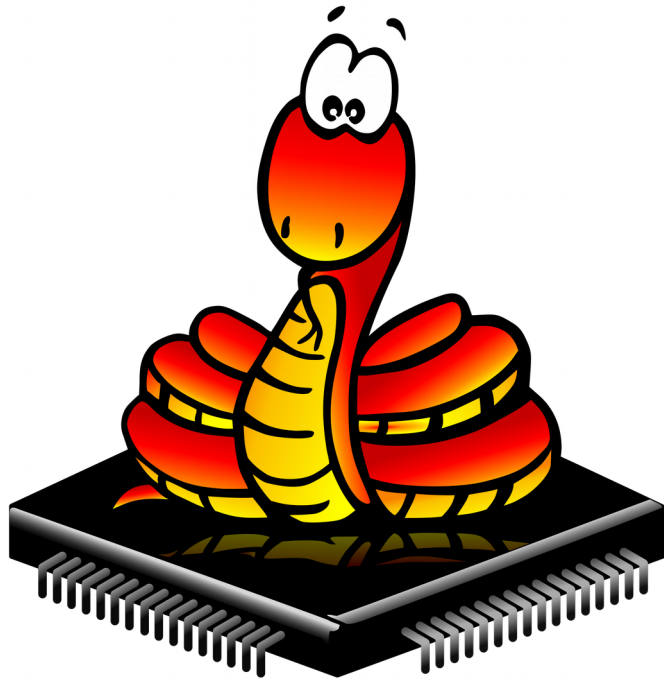
- Messen der Raumtemperatur



<https://pycom.io>



Knoten im Eigenbau: Software



<https://micropython.org>

```
while True:
    temp.start_conversion()
    time.sleep(1)
    curr = temp.read_temp_async()
    ts = int(time.time())
    b = struct.pack("<ii", int(curr*100), ts)
    try:
        lora.send(b)
    except TimeoutError:
        print("LoRa send timed out")
    time.sleep(25)
```



Offenes Netzwerk

www.TheThingsNetwork.org

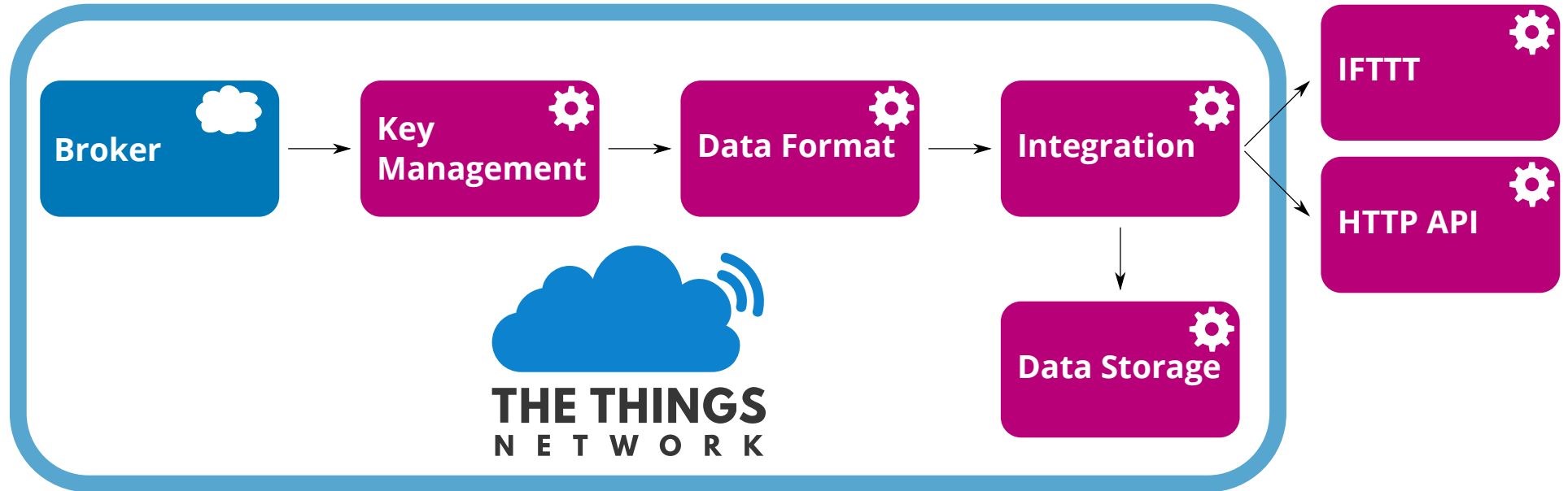


THE THINGS
N E T W O R K

<https://thethingsnetwork.org>



TheThingsNetwork.org



TheThingsNetwork.org: Community Edition

Pro:

- Geringe technische Hürden
- Geteilte Infrastruktur
- Infrastruktur ist auf Github



TheThingsNetwork.org: Community Edition

Pro:

- Geringe technische Hürden
- Geteilte Infrastruktur
- Infrastruktur ist auf Github

Con:

- Anbieter sieht Nutzdaten



Ergebnis

Entering the Danger Zone => Zeigen des graphischen Loggins

Aufbau eines Sensornetzes mit LoRaWAN

Funk für Bereiche, die sich mit WLAN nicht abdecken lassen

Chris Fiege – c.fiege@pengutronix.de

