LPWAN interim
LoRaWAN IID

08/01/2020

Current IID proposition

1. key = LoRaWAN AppSKey
2. cmac = aes128_cmac(key, devEui)
3. IID = cmac[0..7]

Potential issue: LoRa Alliance might refuse to reuse AppSKey

Other proposition

- Based on RFC7217 where the IID is "stable for each subnet":
- RID = F(Prefix, Net_Iface, Network_ID, DAD_Counter, secret_key), where Net_Iface can be DevEUI and Network_ID the LoRaWAN netid.

- How secret_key is setup ?
- Potential issue: will not change over time