LoRaWAN and Public Key Cryptography

Julien Catalano

Kerlink Deputy CTO

LoRa Alliance Technical Committee Vice Chair

Simple. Affordable. Transformative.

Agenda

- LoRaWAN Architecture
- Public Key Cryptography
- Public Key Infrastructure
- Further Explorations

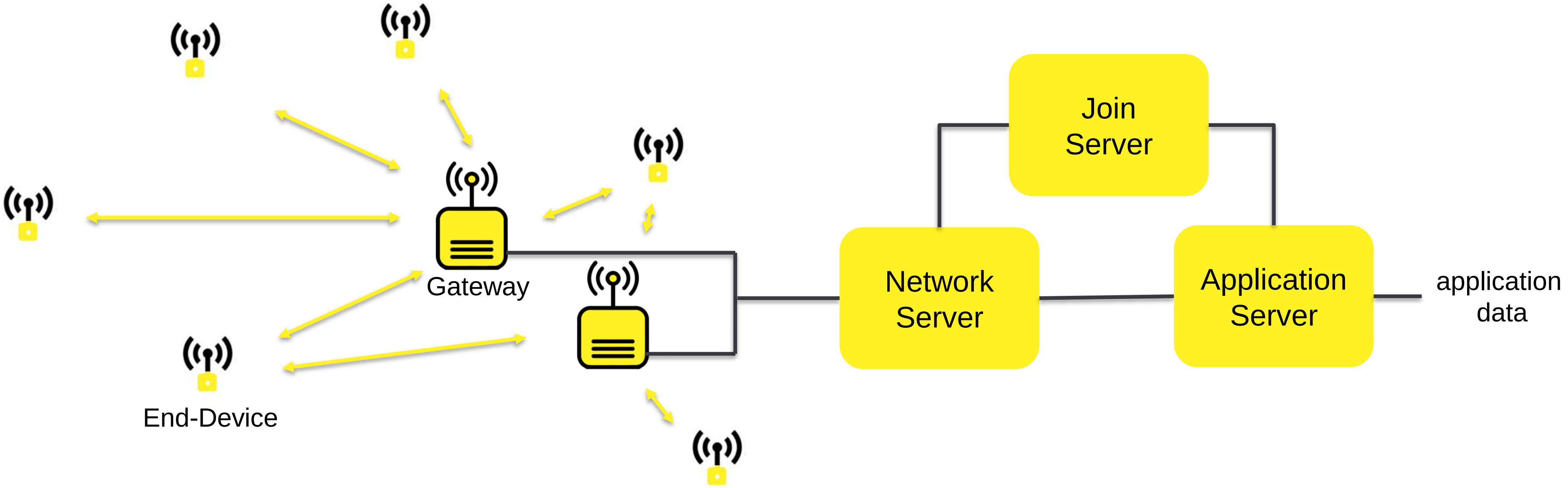
Julien Catalano

kerlink
communication is everything

×

LoRa Alliance®

LoRaWAN® Technical Architecture



LoRaWAN is secured

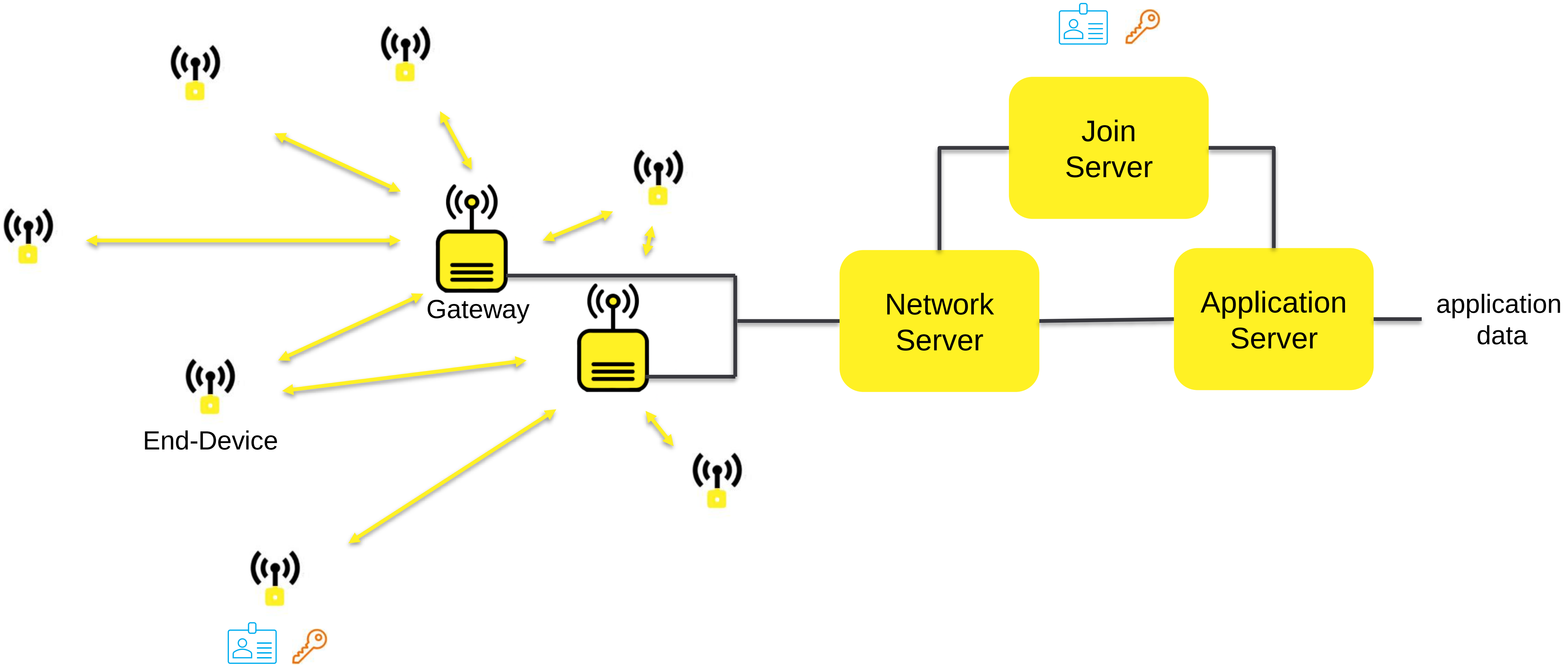
End-to-end encryption

Frame authentication

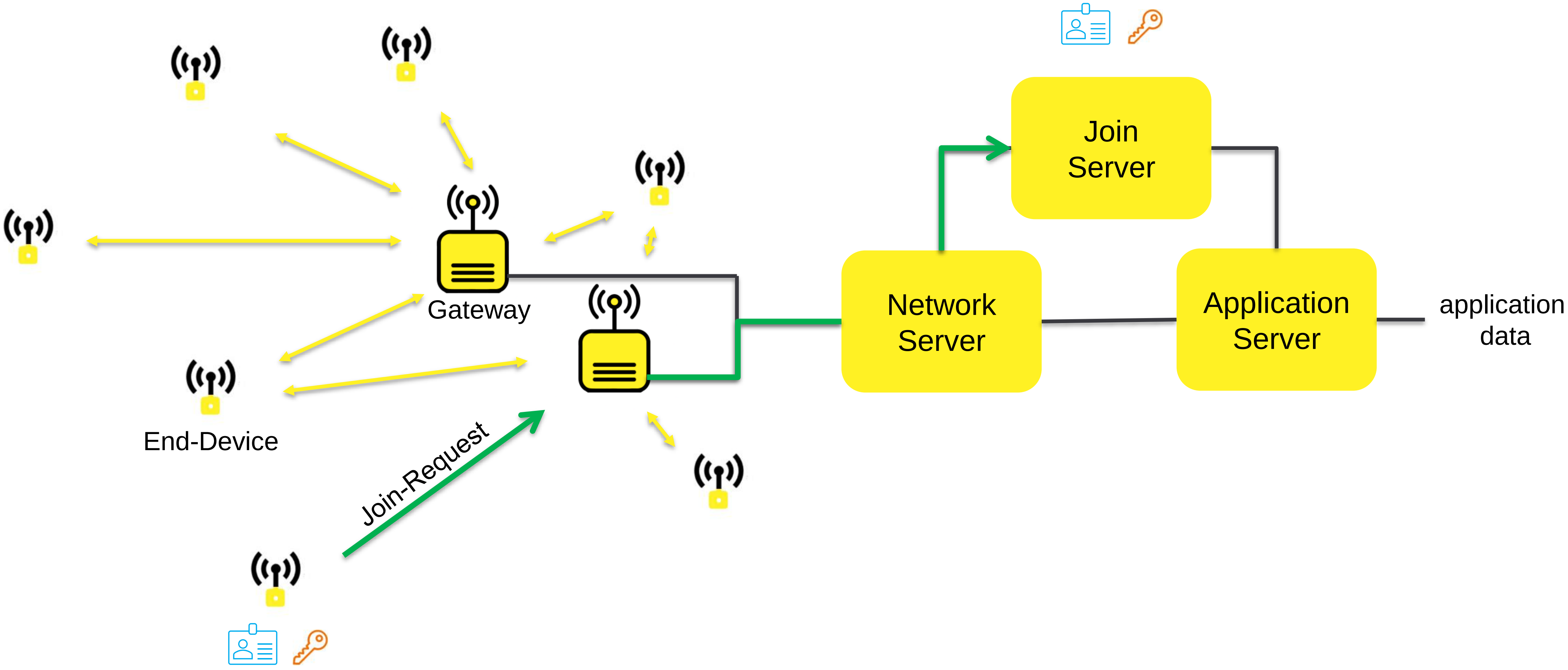
Join Procedure

AES-128 cipher + Crypto agility

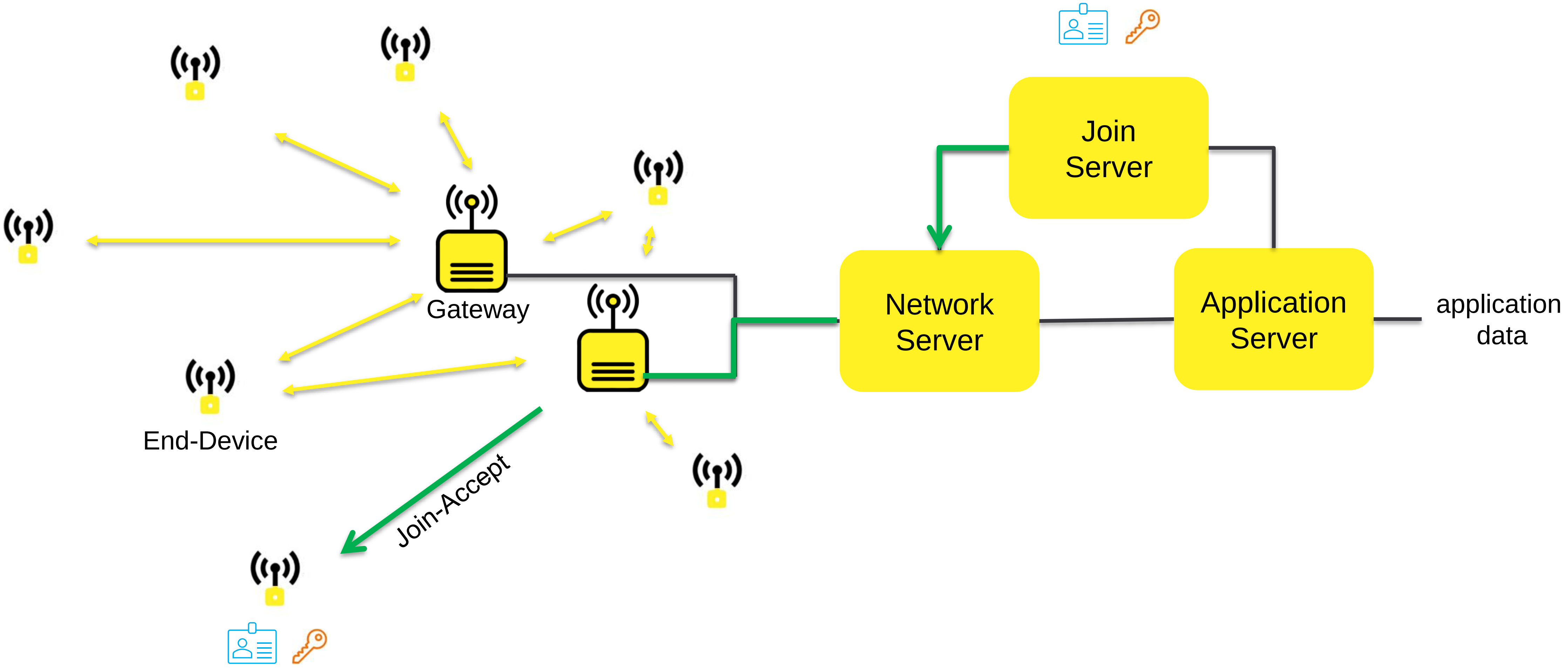
LoRaWAN Join Procedure



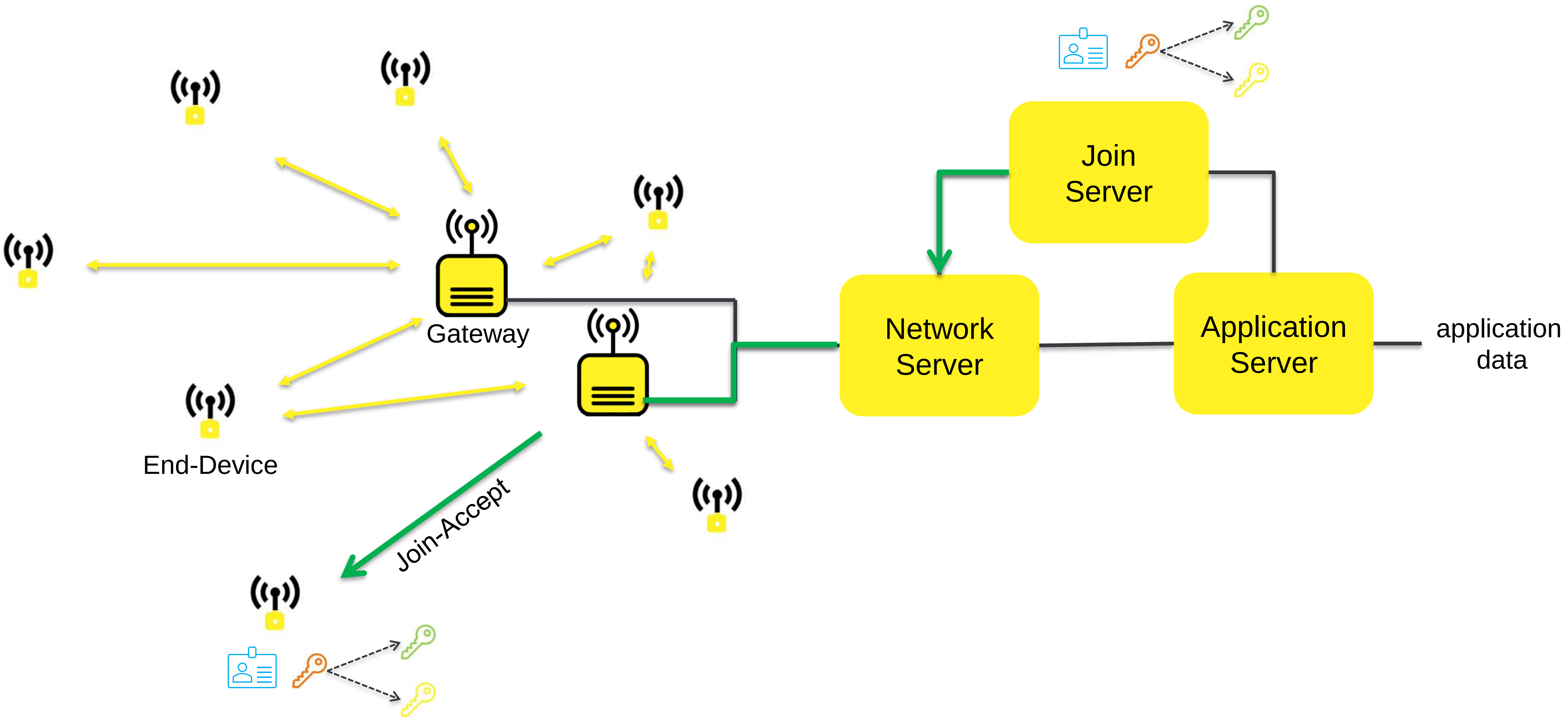
LoRaWAN Join Procedure



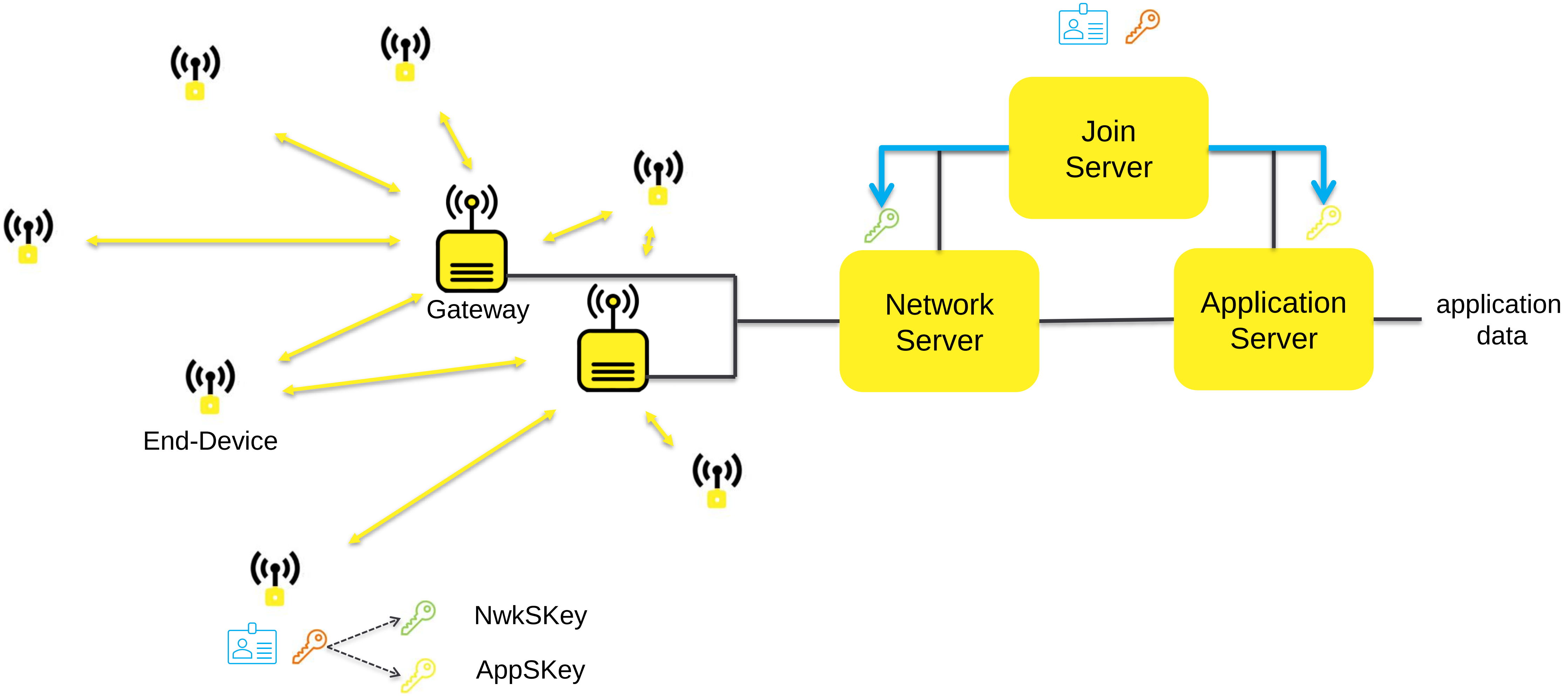
LoRaWAN Join Procedure



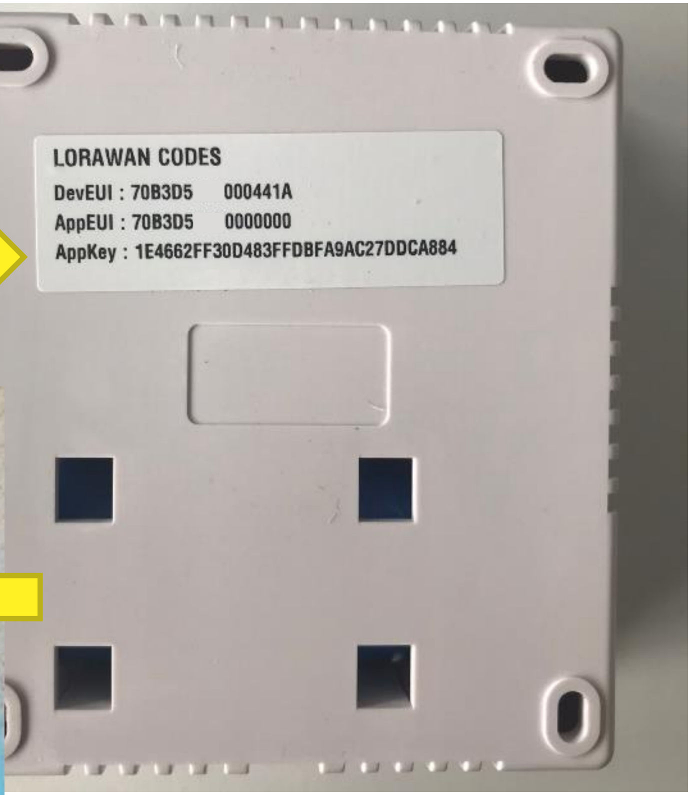
LoRaWAN Join Procedure



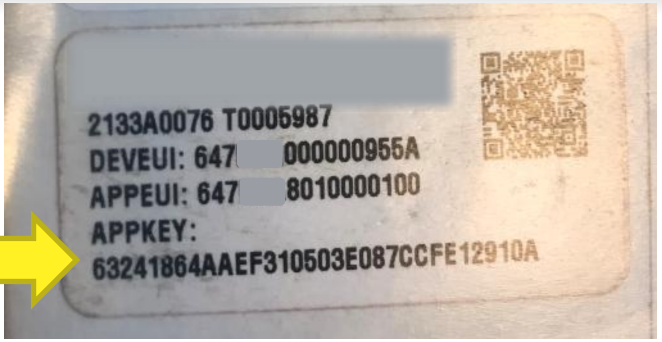
LoRaWAN Join Procedure



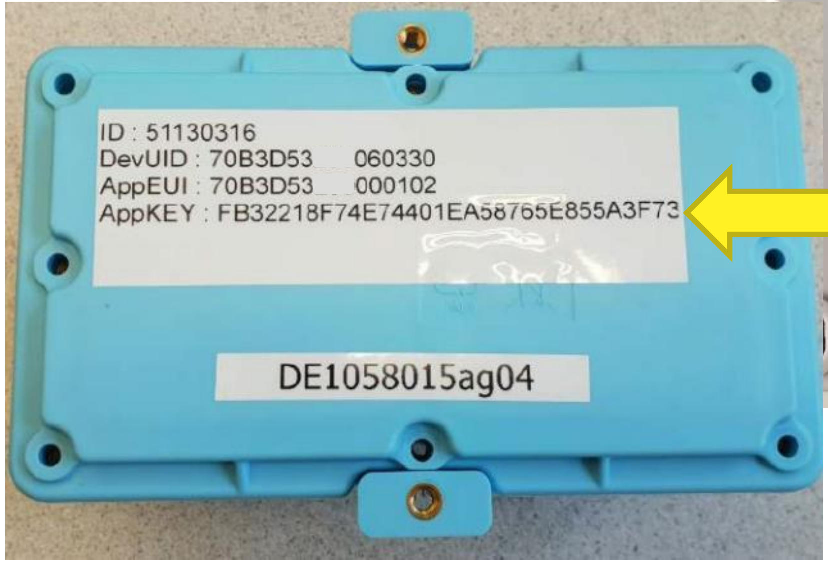
LoRaWAN Provisioning is Complex



LORAWAN CODES
DevEUI : 70B3D5 [redacted] 000441A
AppEUI : 70B3D5 [redacted] 0000000
AppKey : 1E4662FF30D483FFDBFA9AC27DDCA884

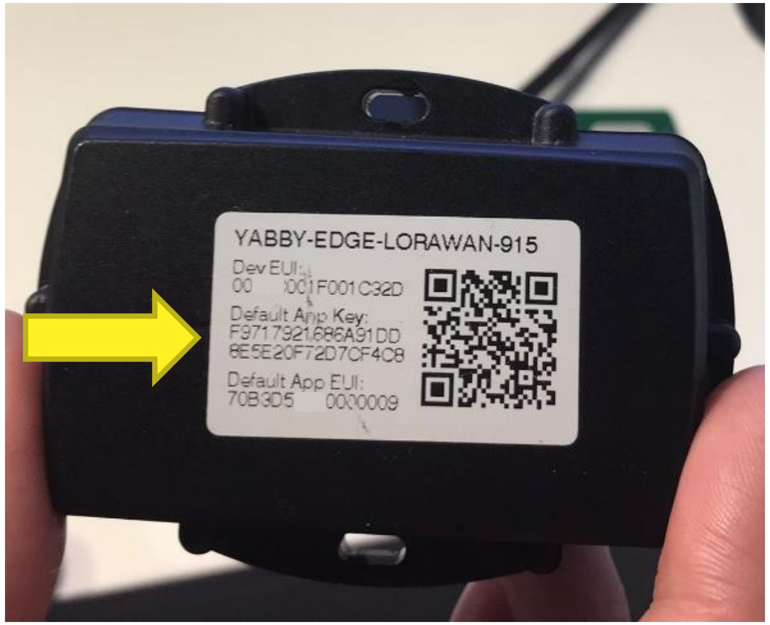


[redacted]
2133A0076 T0005987
DEVEUI: 647[redacted]000000955A
APPEUI: 647[redacted]8010000100
APPKEY:
63241864AAEF310503E087CCFE12910A



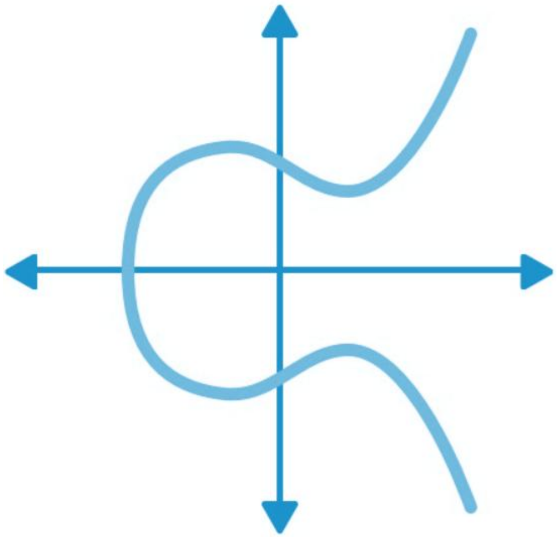
ID : 51130316
DevUID : 70B3D53[redacted]060330
AppEUI : 70B3D53[redacted]000102
AppKEY : FB32218F74E74401EA58765E855A3F73

DE1058015ag04



YABBY-EDGE-LORAWAN-915
Dev EUI:
00[redacted]001F001C32D
Default App Key:
F9717921686A91DD
8E5E20F72D7CF4C8
Default App EUI:
70B3D5[redacted]0000009

Public Key Cryptography in LoRaWAN



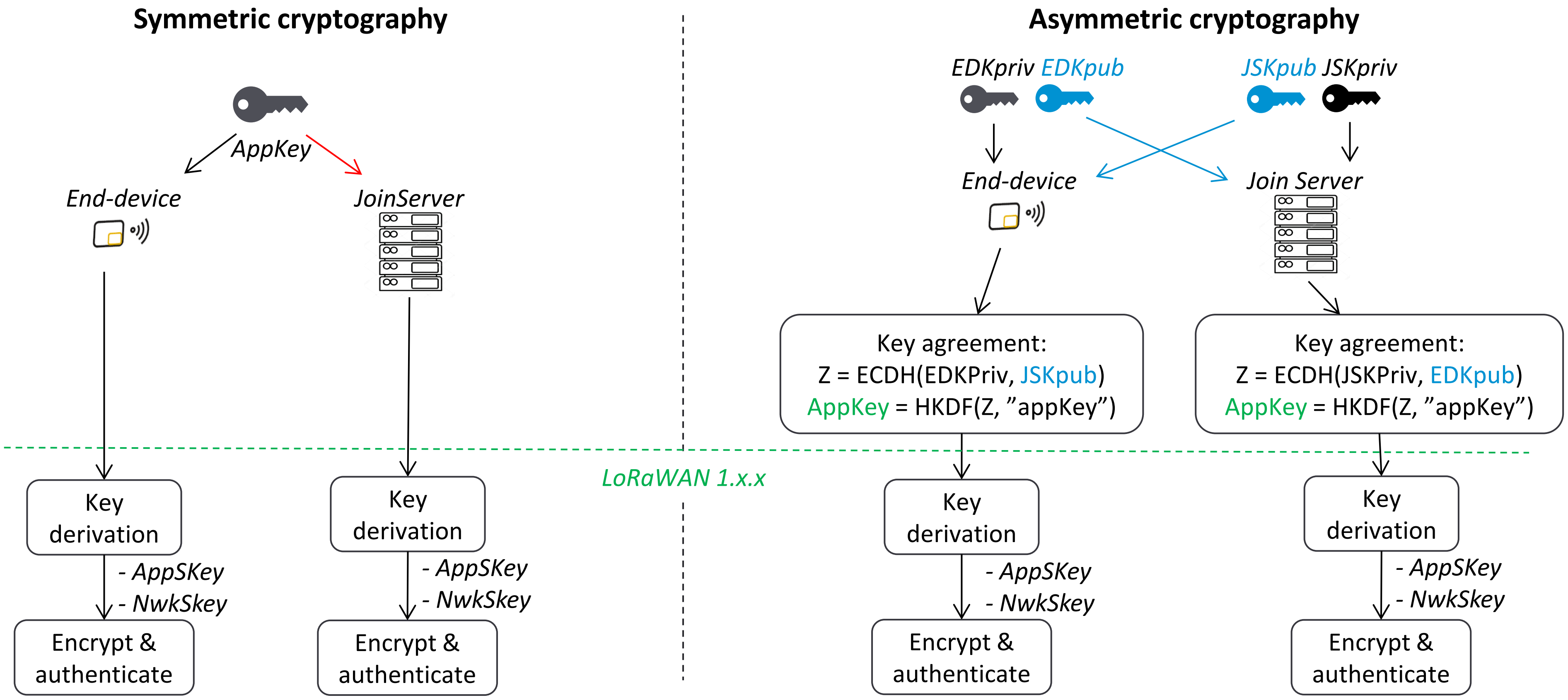
LoRaWAN Root key agreement

Elliptic Curve Cryptography

Asymmetric Cryptography

ECDH

LoRaWAN Root Key Agreement



Simplified diagram

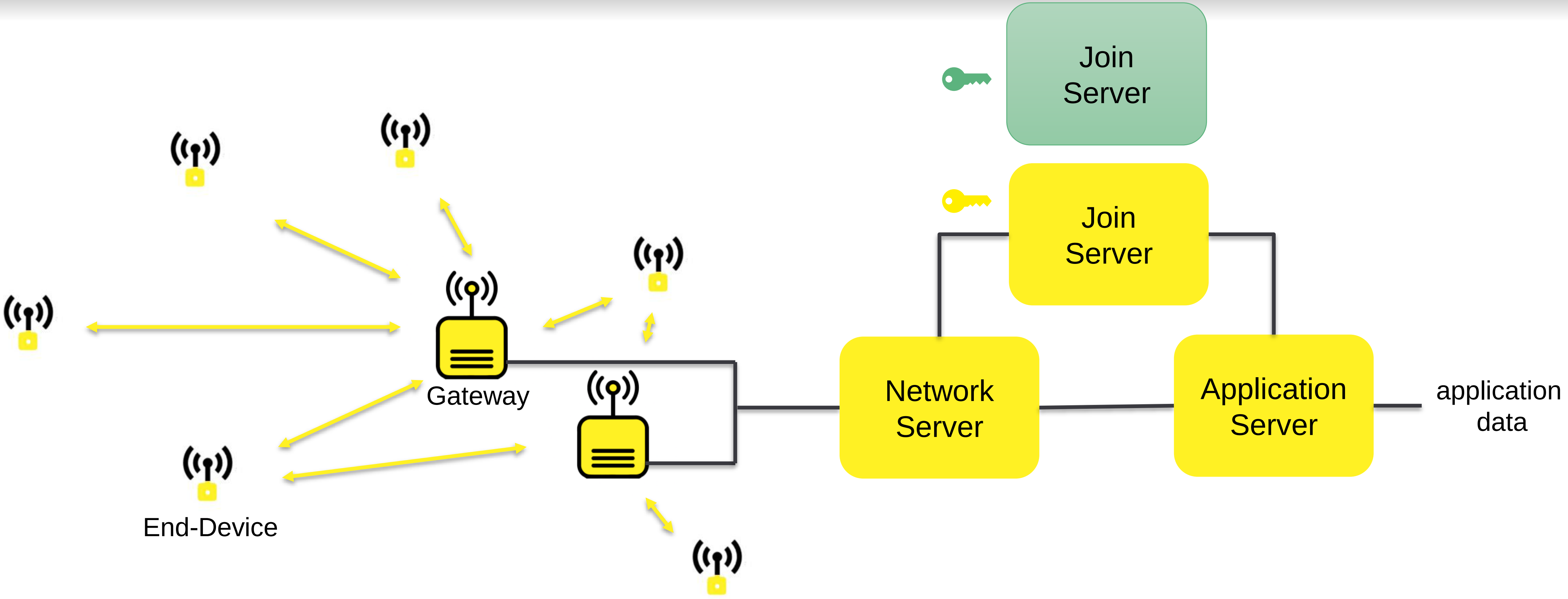
Public Key Infrastructure

Join Server Key Update

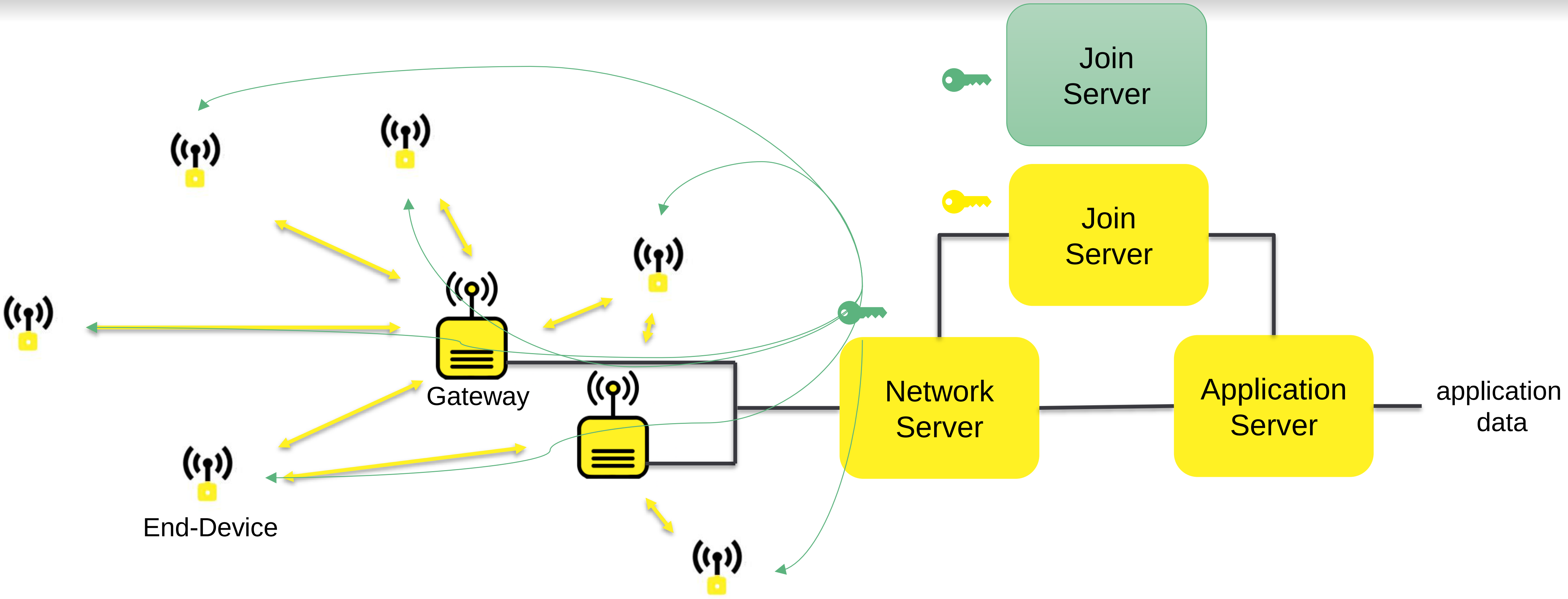
Certificate

DNS

Join Server Key Update

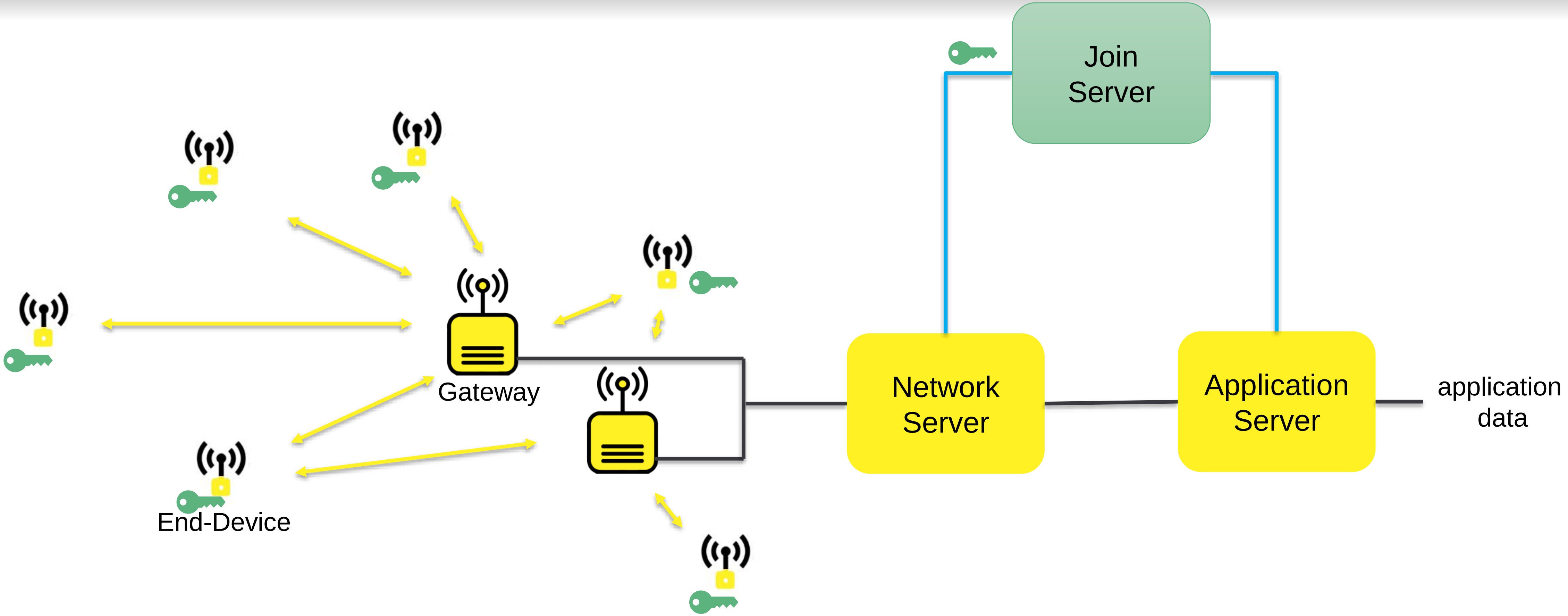


Join Server Key Update



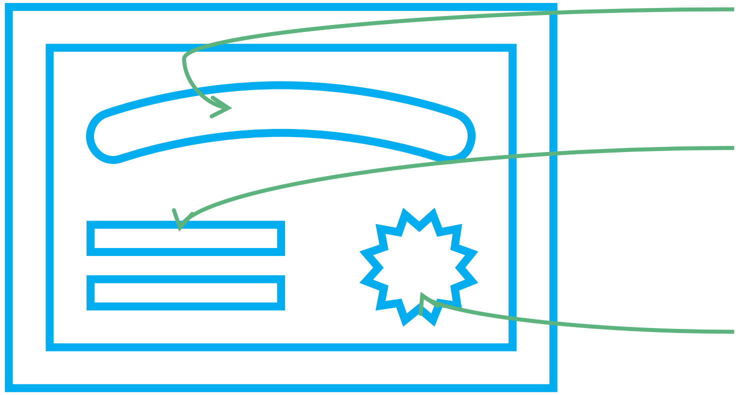
- Public Key size
  - secp256r1: 33B
  - Ed25519: 32B
- Same JS key for all end-devices
  - Broadcast
  - Multicast (FUOTA)

Join Server Key Update



- Public Key size
  - secp256r1: 33B
  - Ed25519: 32B
- Same JS key for all end-devices
  - Broadcast
  - Multicast (FUOTA)

IoT Certificates



Name: EUI

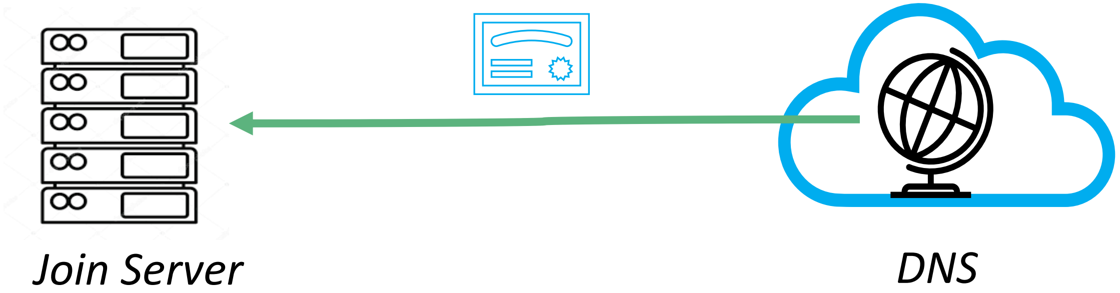
Public Key

Signature of Authority

- CBOR Encoded X.509 Certificates (C509 Certificates) [draft-ietf-cose-cbor-encoded-cert]

RFC7925 profiled C509 certificate Typ. 140B

Domain Name System (DNS)



- DNS DANE / DANCE: store certificate, key or hash in a DNS record
  - draft-ietf-dance-client-auth + RFC6698 (DANE)

```
7076FF0000D01234._device.lorawan.net. IN TLSA (
    3 1 0 025bc3cab35afc217c4fdae34da9f51c
          92af4aa3675b5491cc835bd38a06864cd0 )
```

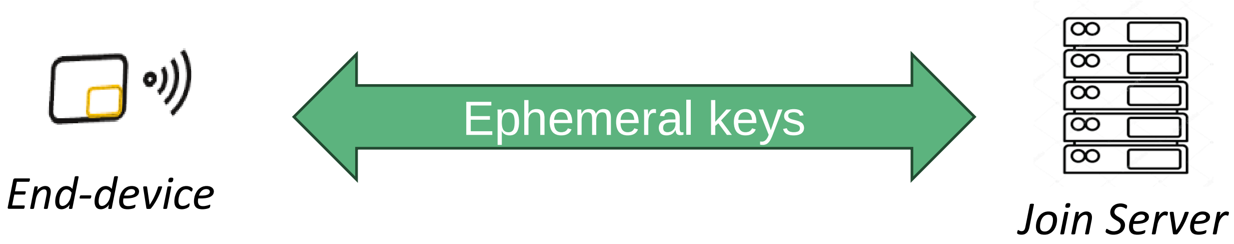
Further Explorations

Ephemeral keys

Post Quantum Cryptography

Crypto Agility

Ephemeral Keys – ECDHE



- Exchange of authenticated ephemeral keys, *i.e.*, **certificates**
- Forward secrecy: previous communication are not compromised, even if secrets leaks

Post Quantum Cryptography

- Elliptic Curve Cryptography is considered weak with quantum computers
- Current status
  - PQC algorithms are in construction
  - Public keys are larger than ECC

- Crypto agility allows to get ready when switching to quantum resistant keys.

Conclusion

LoRaWAN is secured

Key agreement using Public Key Cryptography

Post Quantum Cryptography

Join Procedure

Certificate

Crypto Agility