LoRa® Alliance

Wide Area Networks for IoT

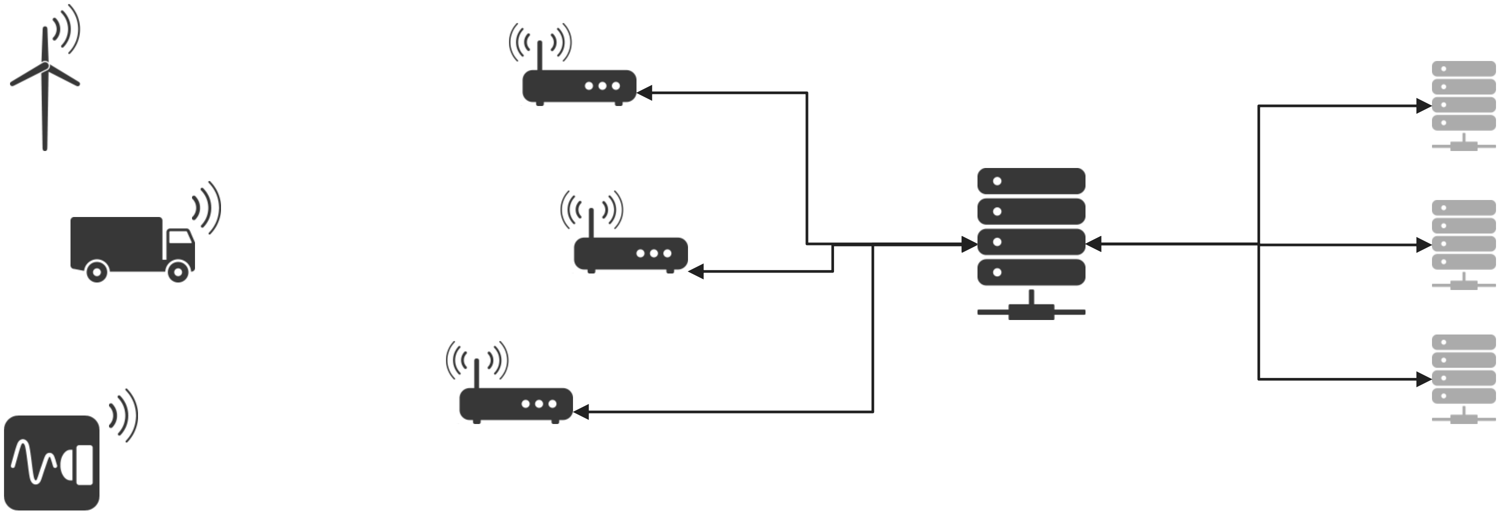
LoRaWAN™ - SECURITY a comprehensive insight

Pierre Girard, Gemalto, Solution Security Expert

Agenda

- LoRaWAN security
- Security deployment examples

LoRaWAN architecture



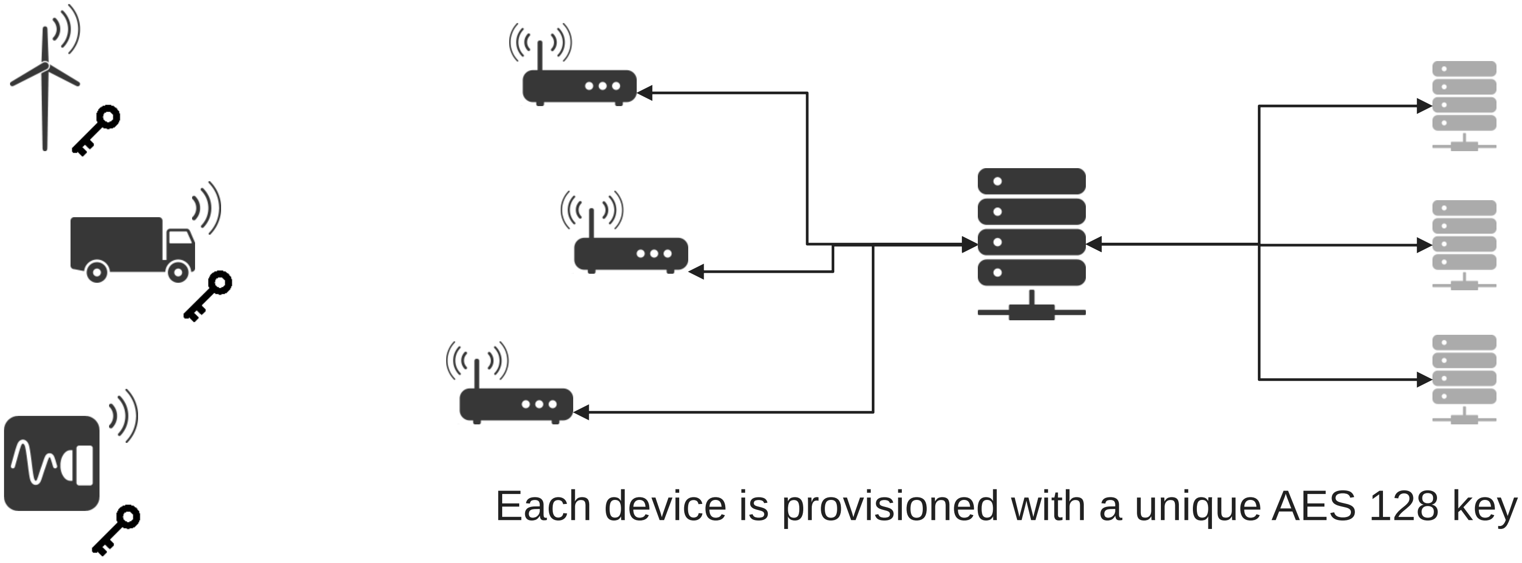
Devices

Gateways

LoRa network server

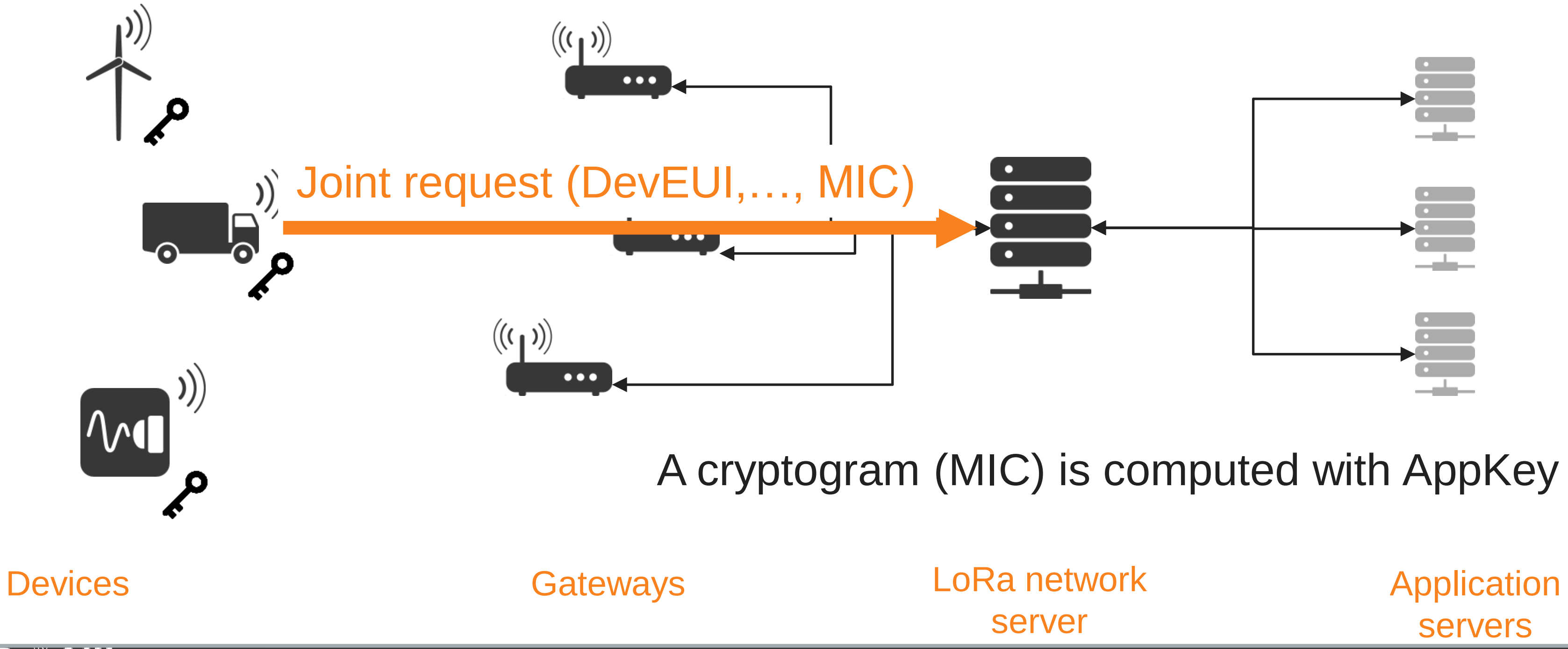
Application servers

LoRaWAN security



Each device is provisioned with a unique AES 128 key : AppKey

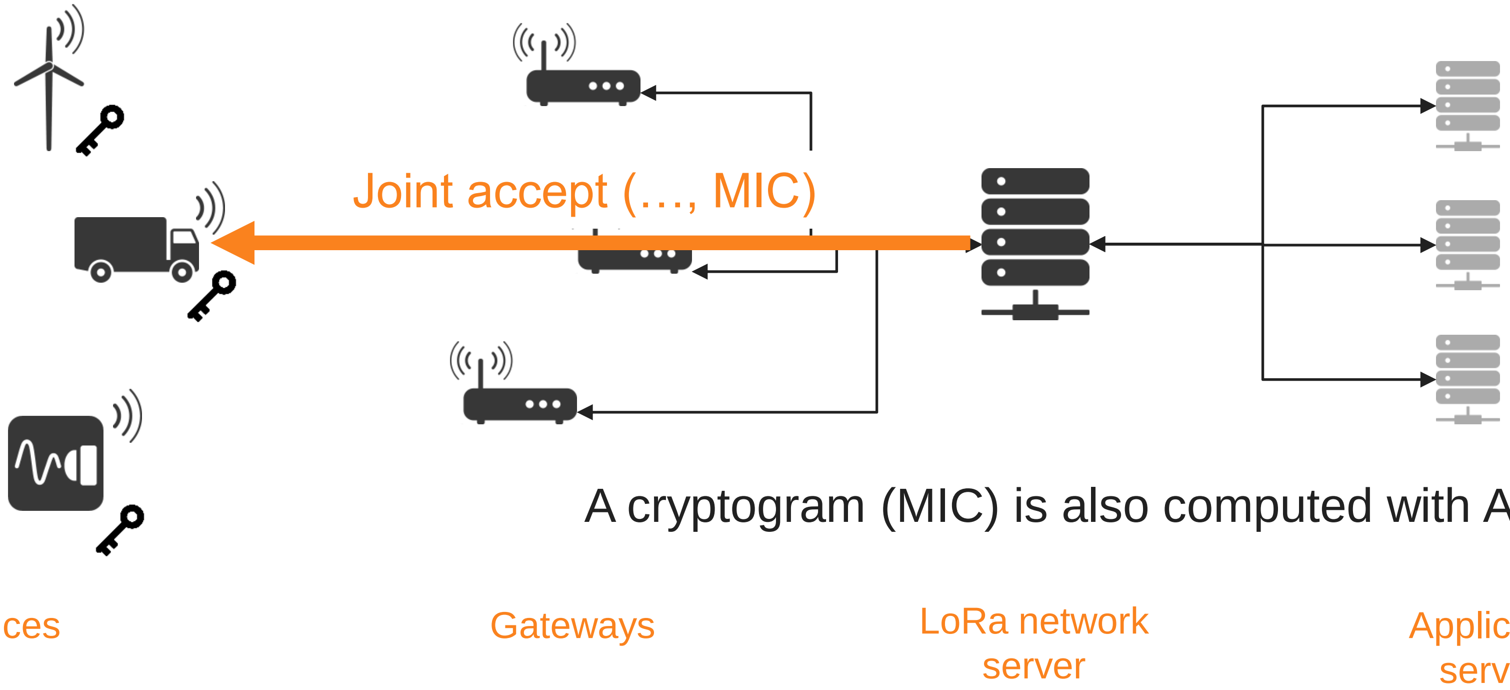
LoRaWAN security: network connection



Joint request (DevEUI,…, MIC)

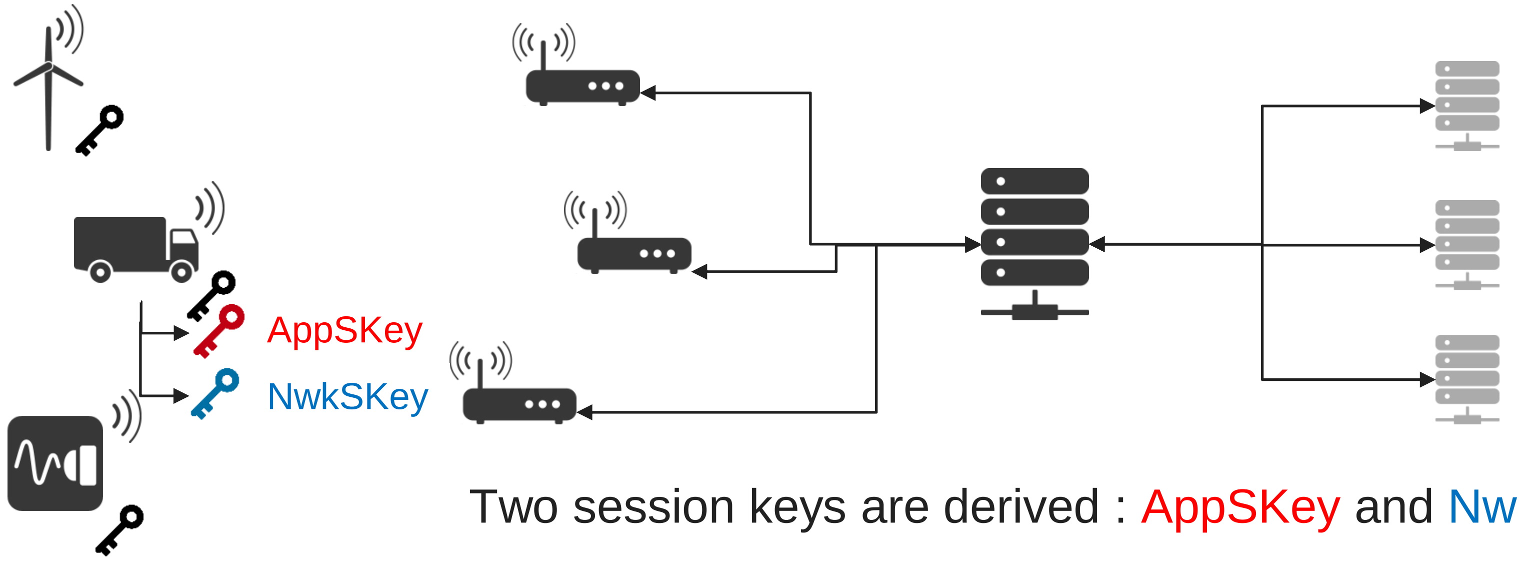
A cryptogram (MIC) is computed with AppKey

LoRaWAN security: network connection



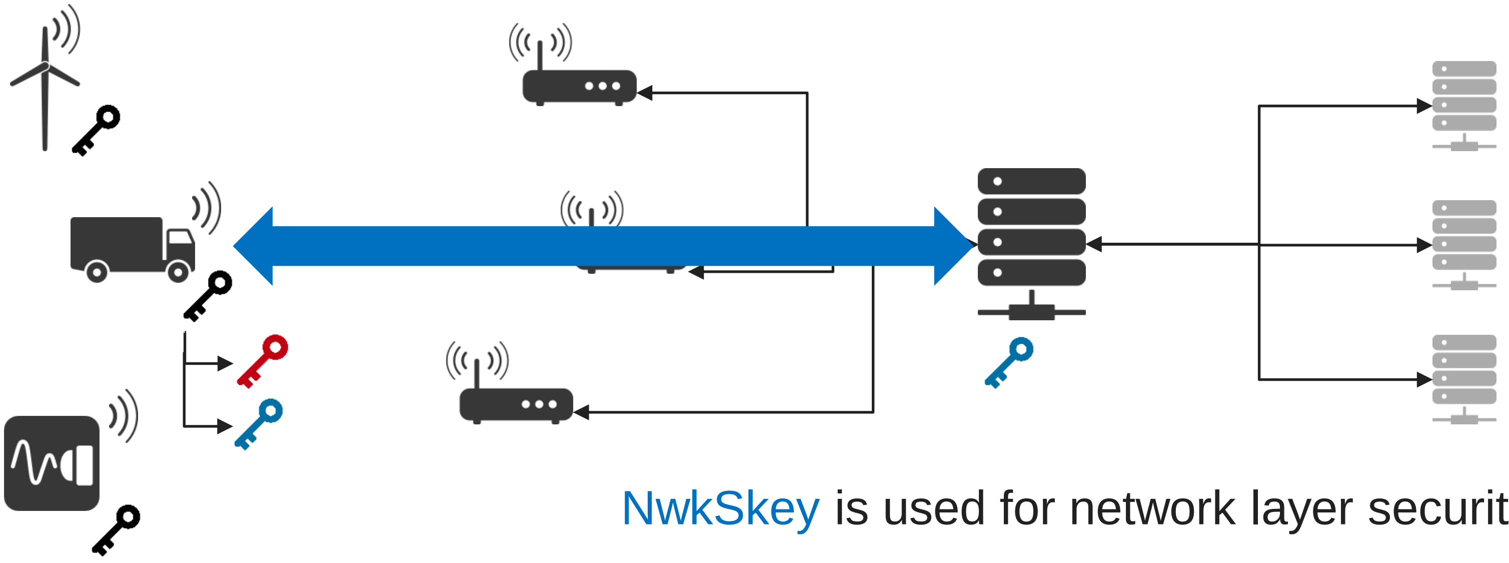
A cryptogram (MIC) is also computed with AppKey

LoRaWAN security: network connection



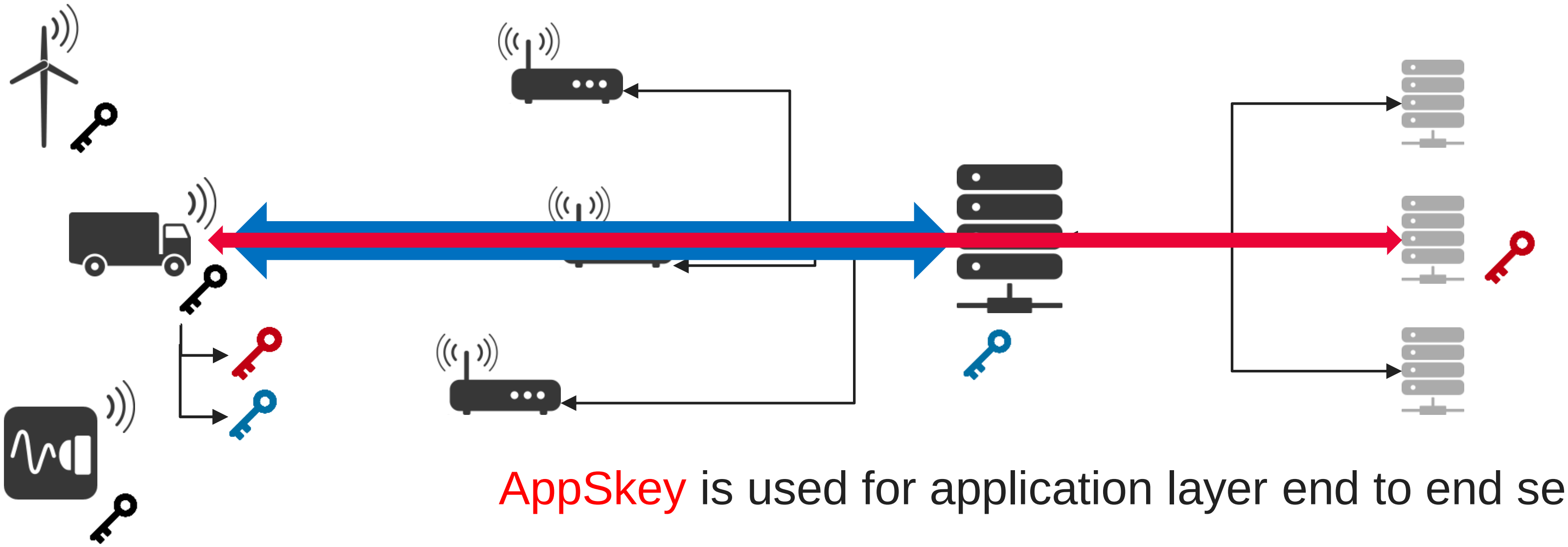
Two session keys are derived : AppSKey and NwkSKey

LoRaWAN security: network connection



NwkSkey is used for network layer security

LoRaWAN security: network connection



AppSkey is used for application layer end to end security

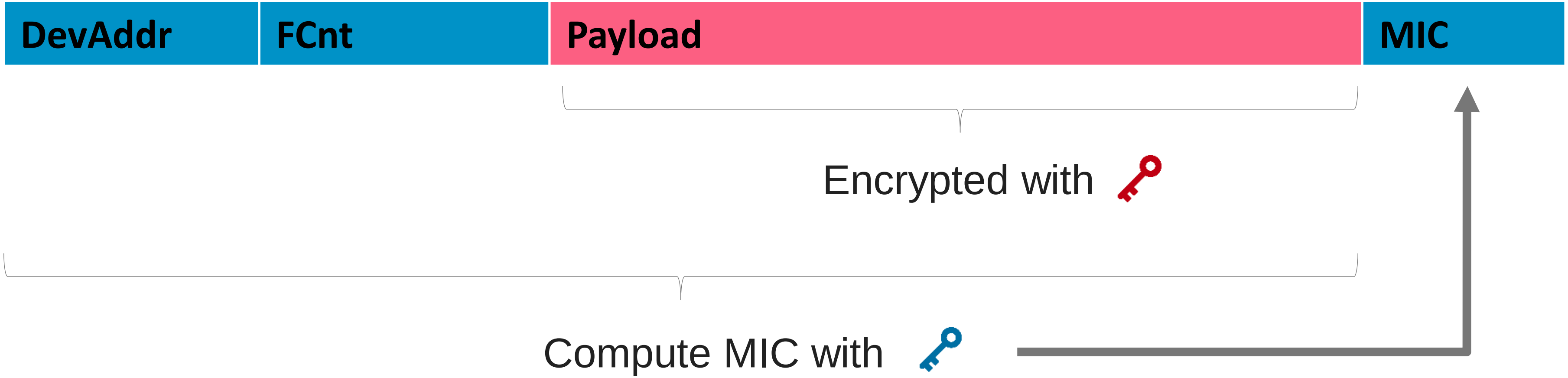
Devices

Gateways

LoRa network server

Application servers

LoRaWAN frame content for payloads



DevAddr | FCnt | Payload | MIC

Encrypted with 🔑

Compute MIC with 🔑

LoRaWAN security takeover

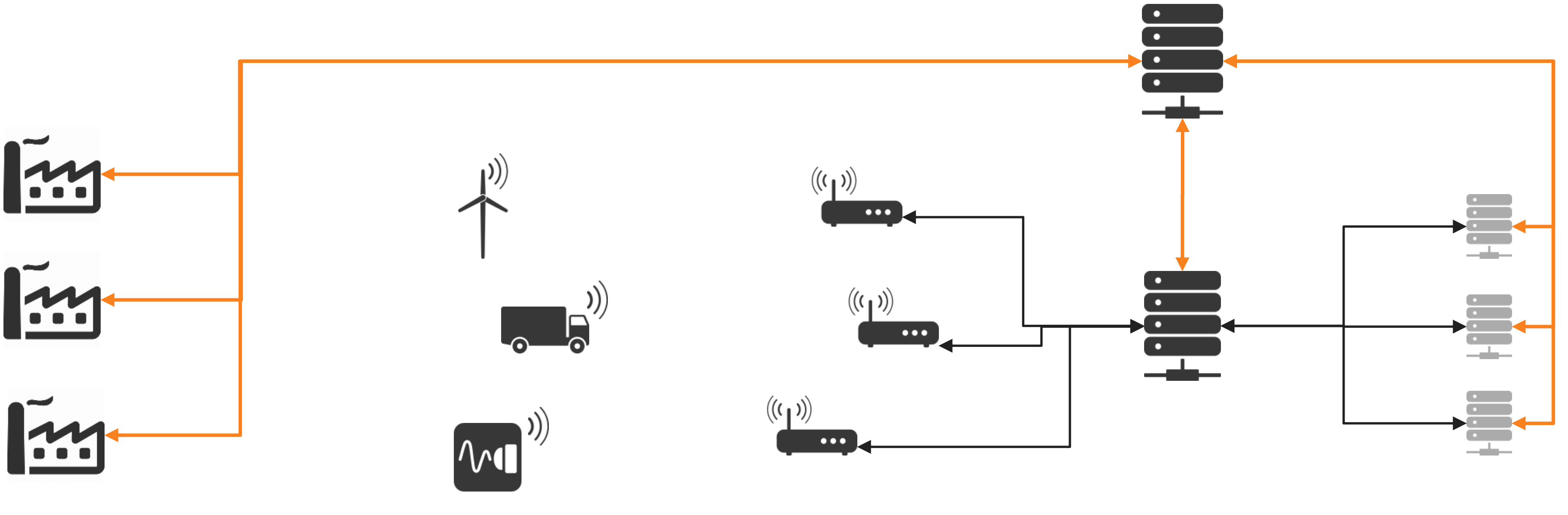
- Security has been built-in from version 1.0
- Based on proven cryptography
    - AES for encryption and MAC
- End-to-end encryption is a strong value-add

Agenda

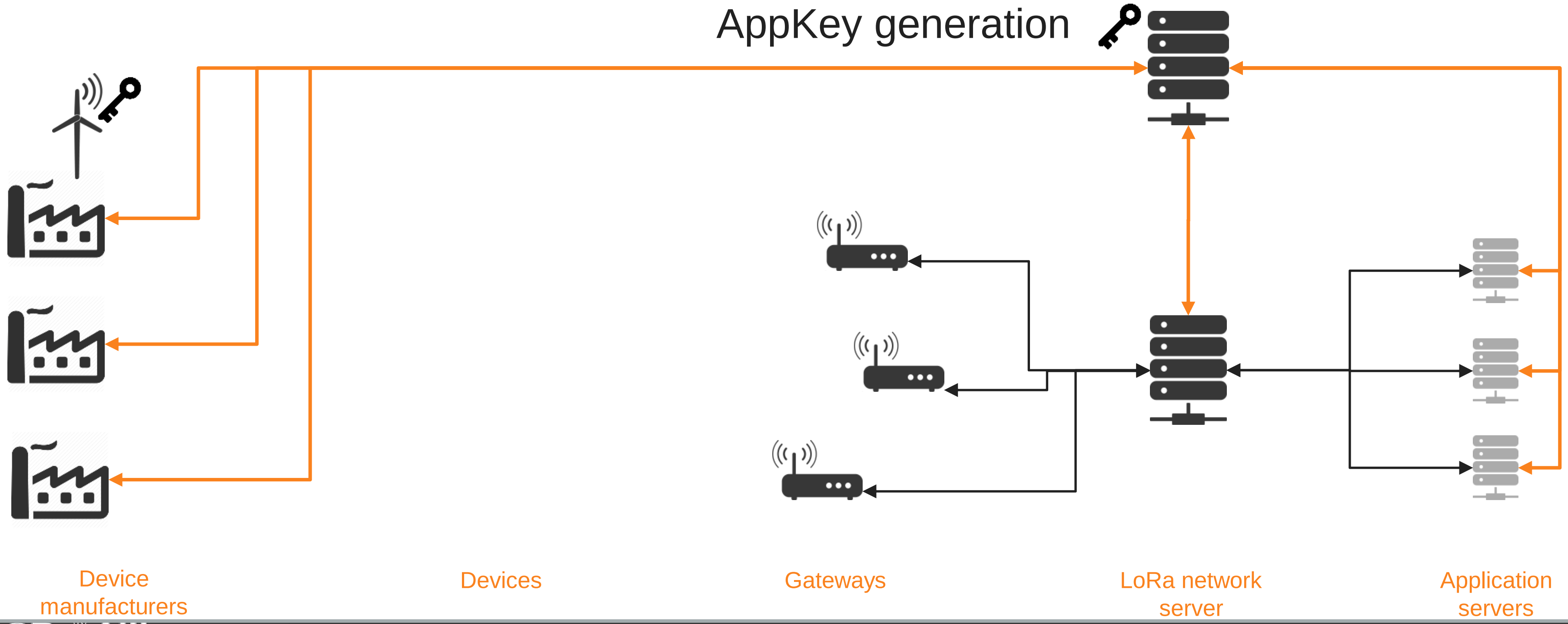
- LoRaWAN security

- Security deployment examples

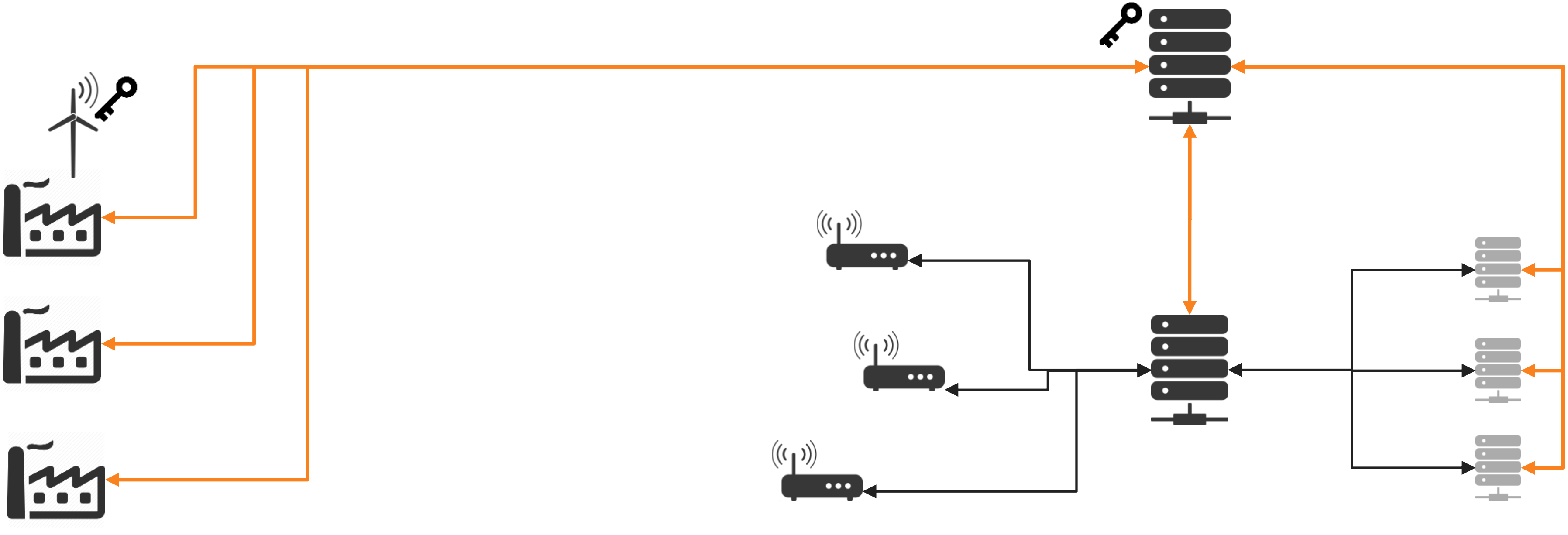
Background links for security deployment



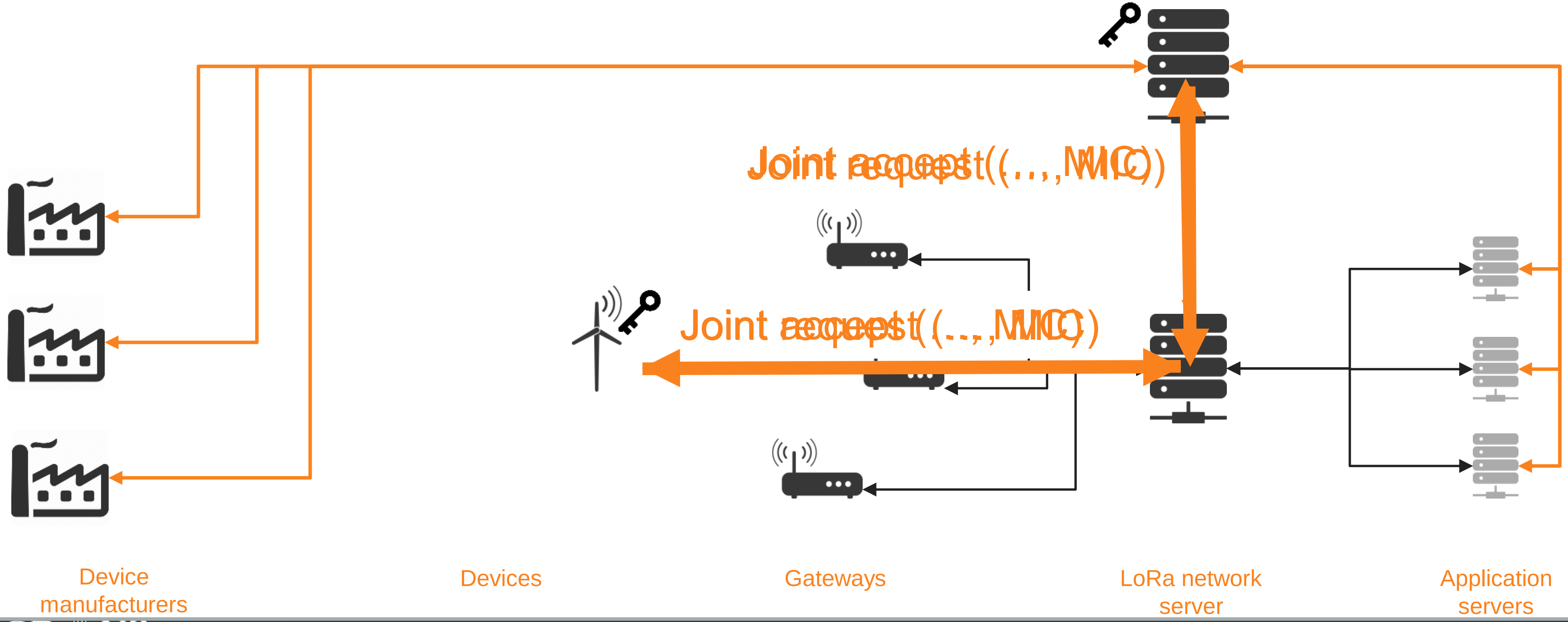
Device provisioning



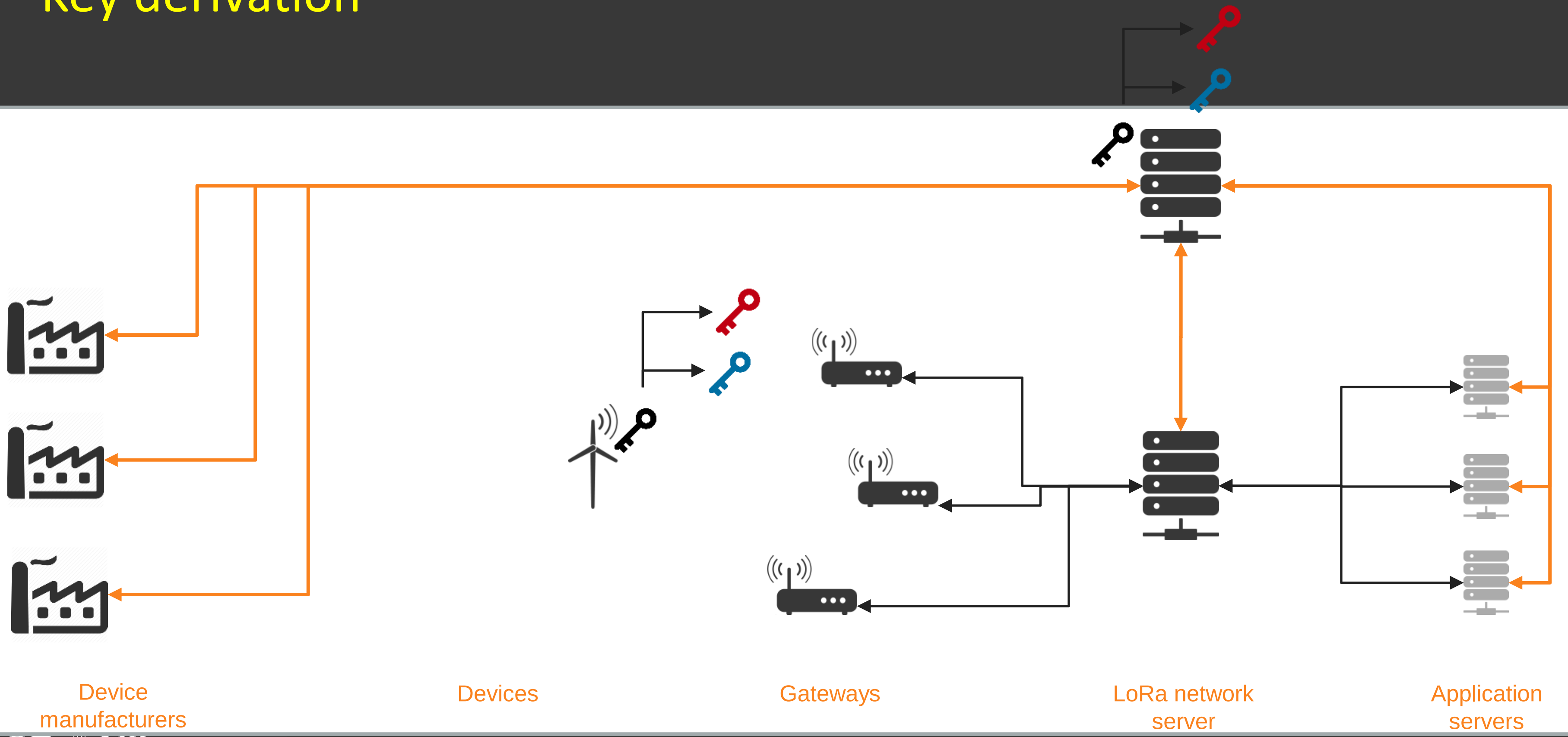
Device provisioning



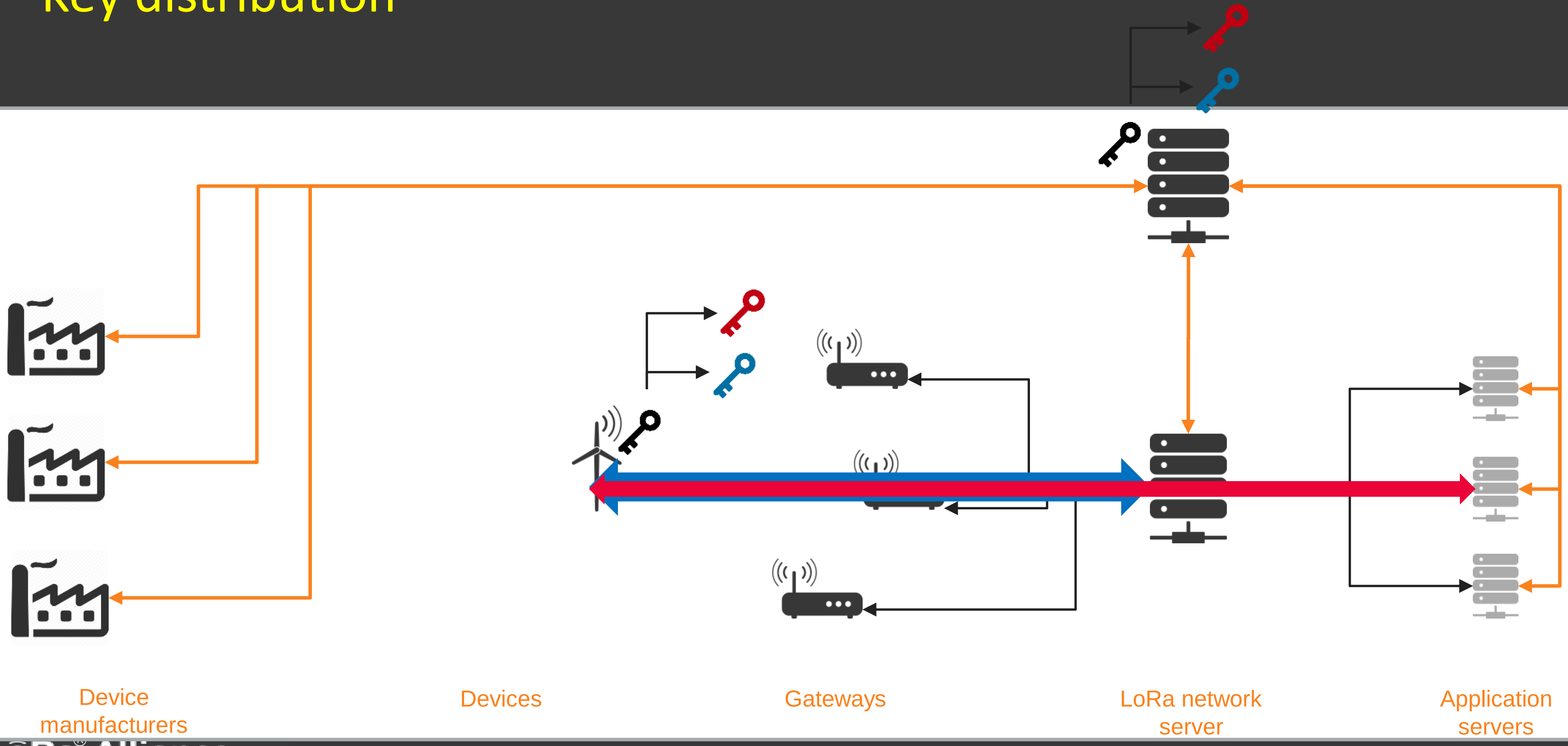
Network connection



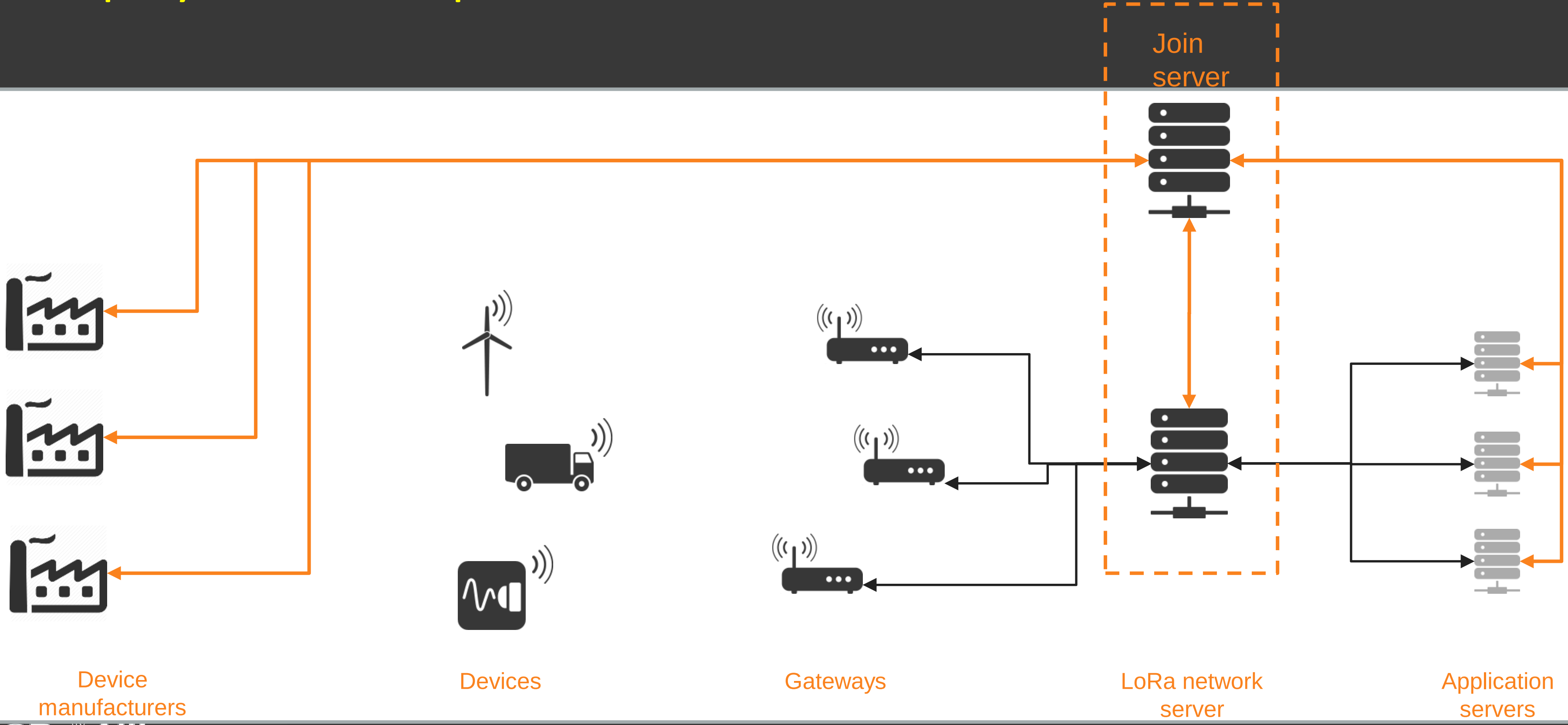
Key derivation



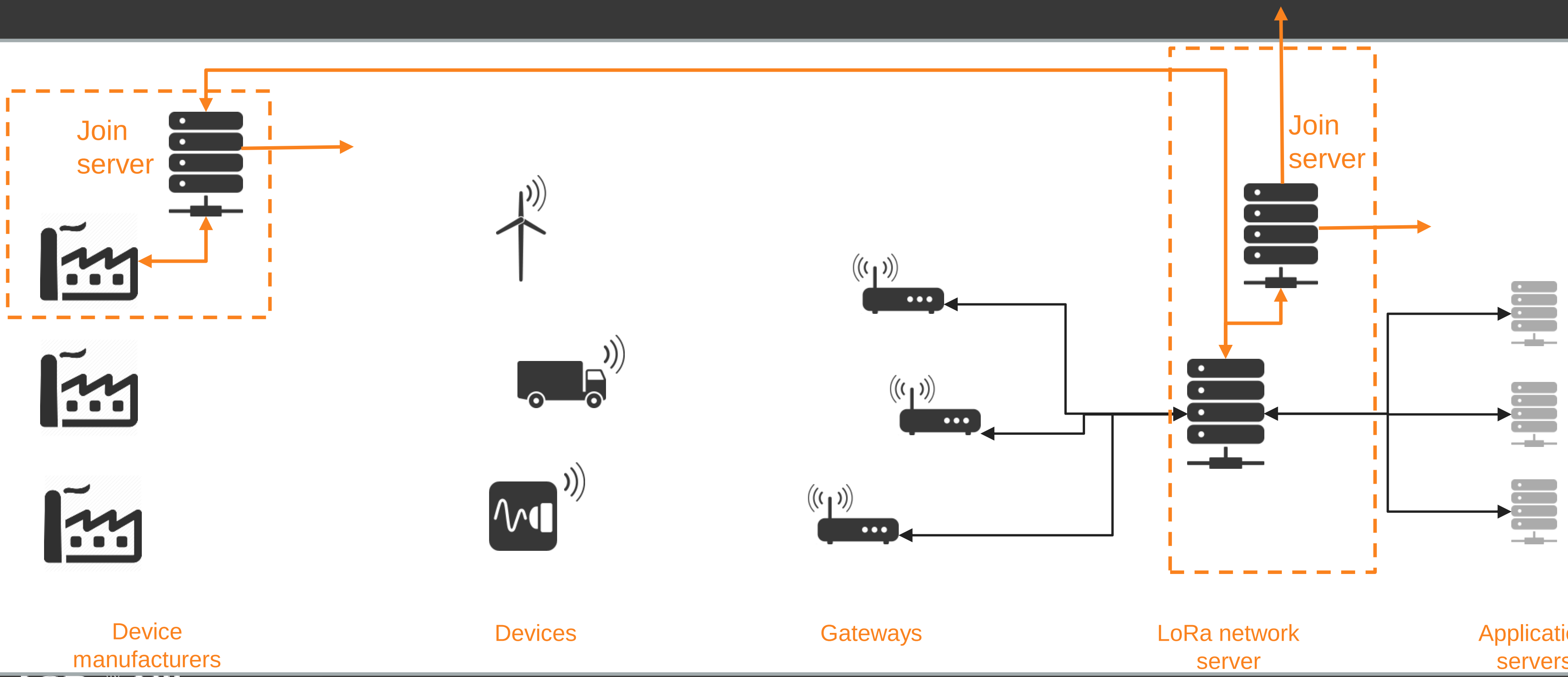
Key distribution



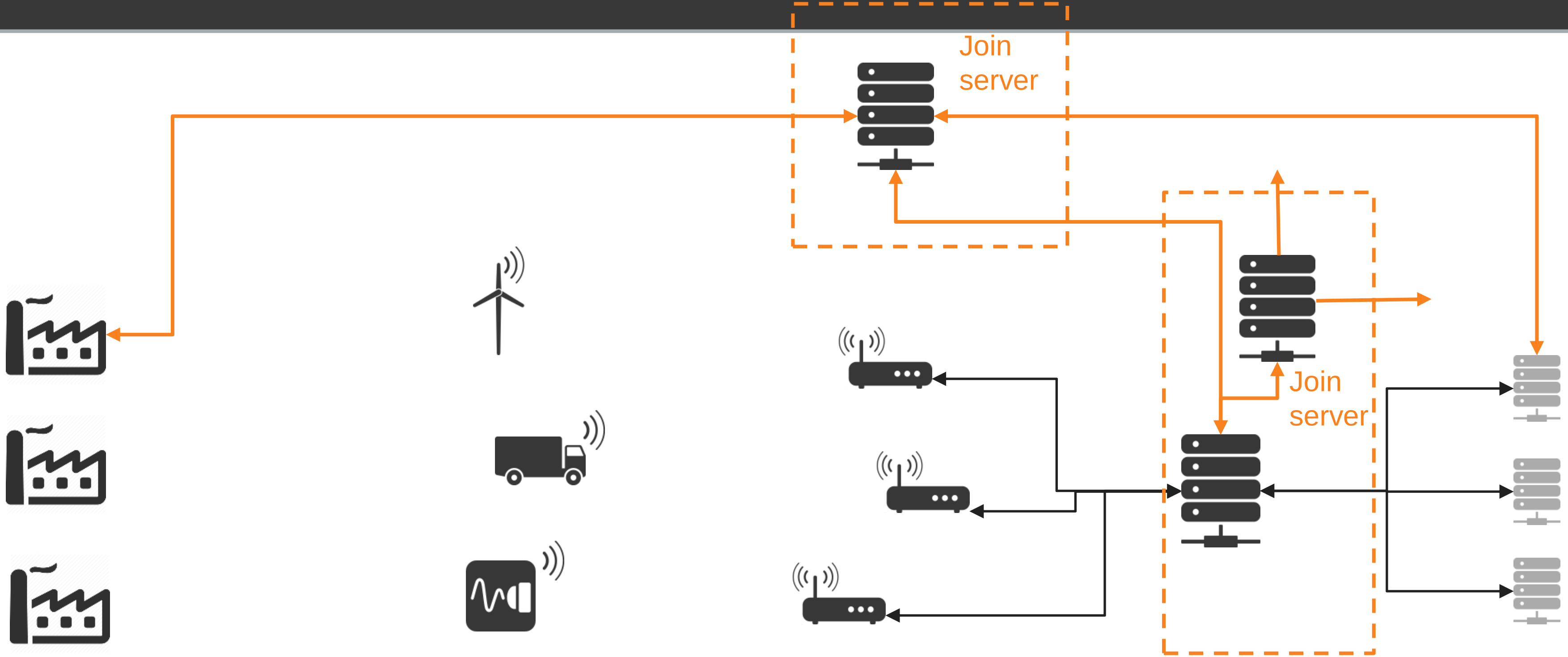
Deployment example 1



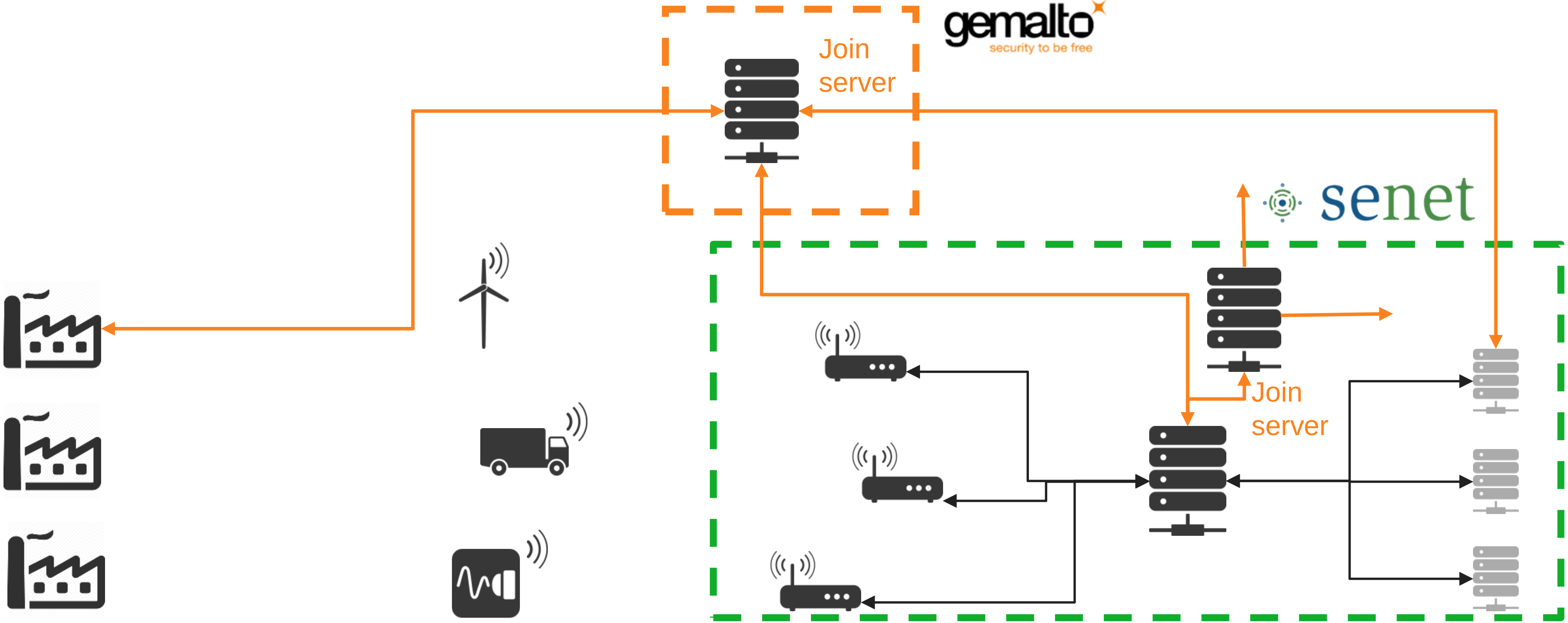
Deployment example 2



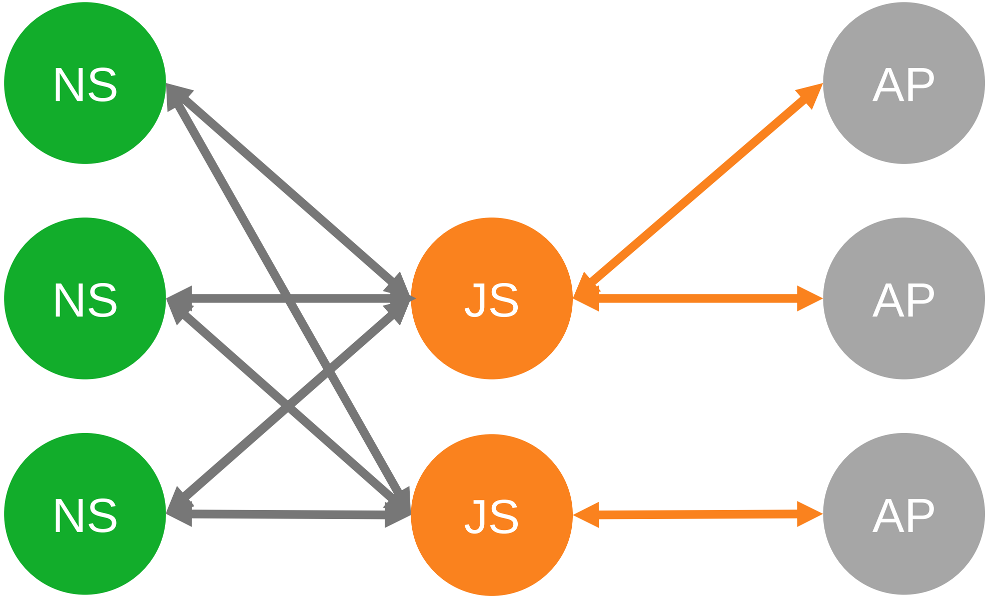
Deployment example 3



Gemalto – Senet demonstration



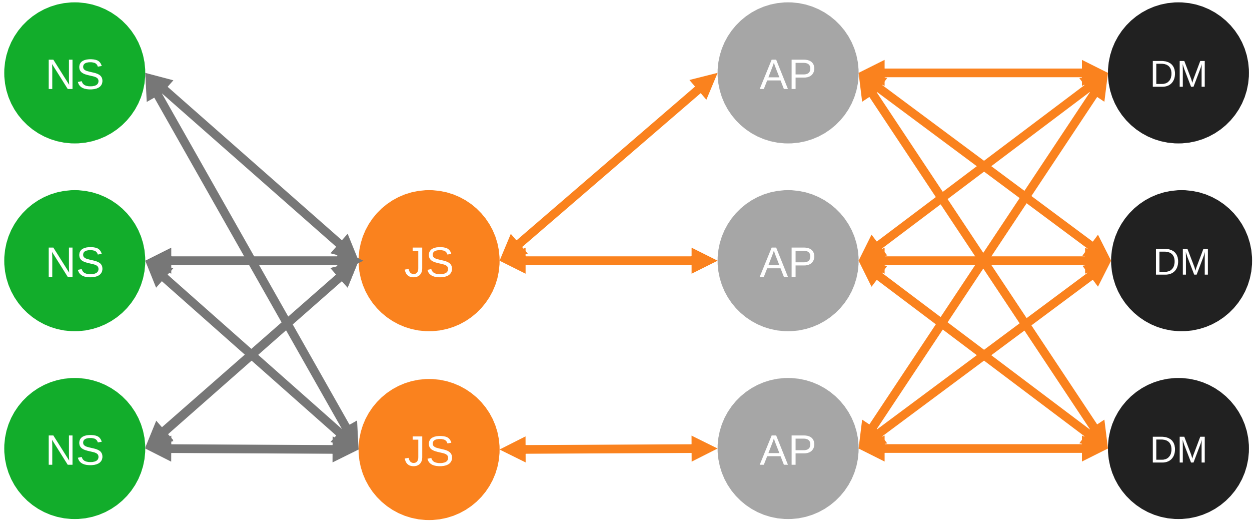
Key provisioning by Application provider



NS: Network Server – AP: Application Server – JS: Join Server

⟷ Link for key prov.

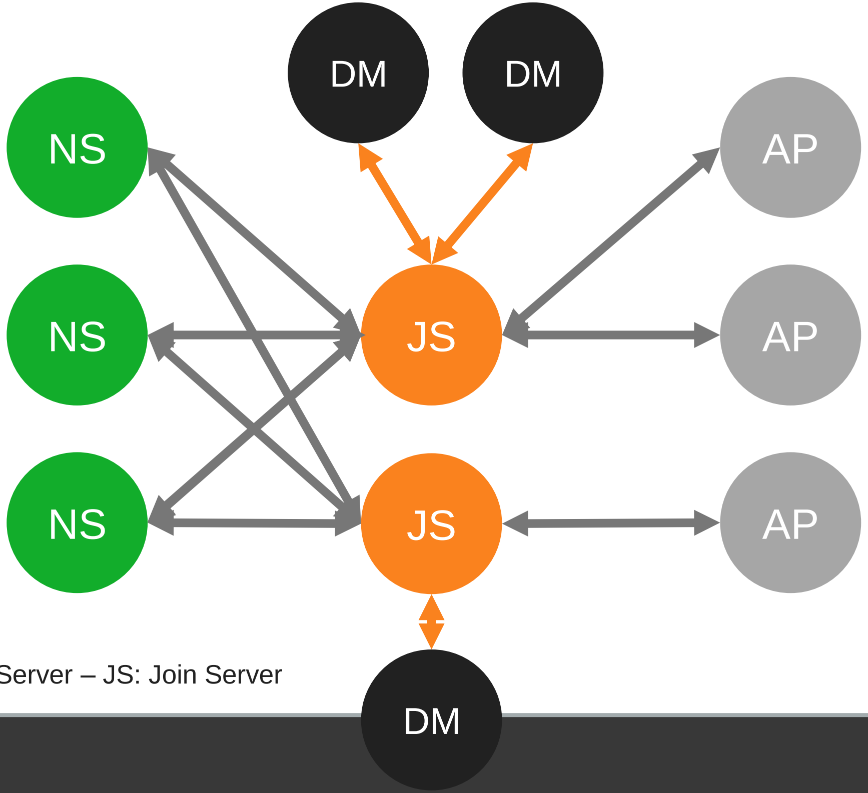
Toward full generic devices



NS: Network Server – AP: Application Server – JS: Join Server

⟷ Link for key prov.

Toward full generic devices



NS: Network Server – AP: Application Server – JS: Join Server

⟷ Link for key prov.

Take away

- LoRaWAN technology has strong security built-in
- Deployments schemes are flexible
- It’s possible to minimize the key provisioning operations

LoRa® Alliance

Wide Area Networks for IoT

Thank you – Together we make the IoT happen!

LoRa-Alliance.org