Low Power Wide Area Networks security

Sophia-Antipolis, December 9, 2015
Pierre Girard, Security Solution Expert

Introduction

- LPWAN technologies are booming
- Main drivers
  - Low cost
  - Low power consumption
- High trust level needs to be maintained

Why trust in IoT ?

- Management of sensitive devices
  - Valve, pump, door, engine, …
- Management of sensitive transactions
  - Energy: (not) producing, (not) consuming, storing …
  - X as a Service: cleaning, manufacturing, flying …
- Management of sensitive data
  - Location / presence, behavior / consumption patterns, …

IoT will redefine your business model …

… and you want to protect it !

Main security requirements

- Device / network mutual authentication
- End-to-end applicative level security

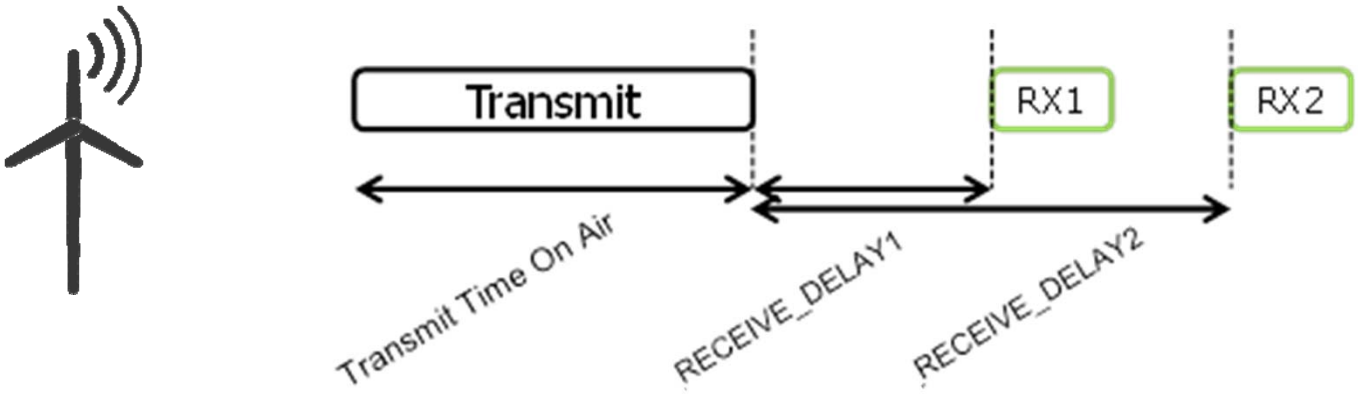
Business as usual

Business as usual ?

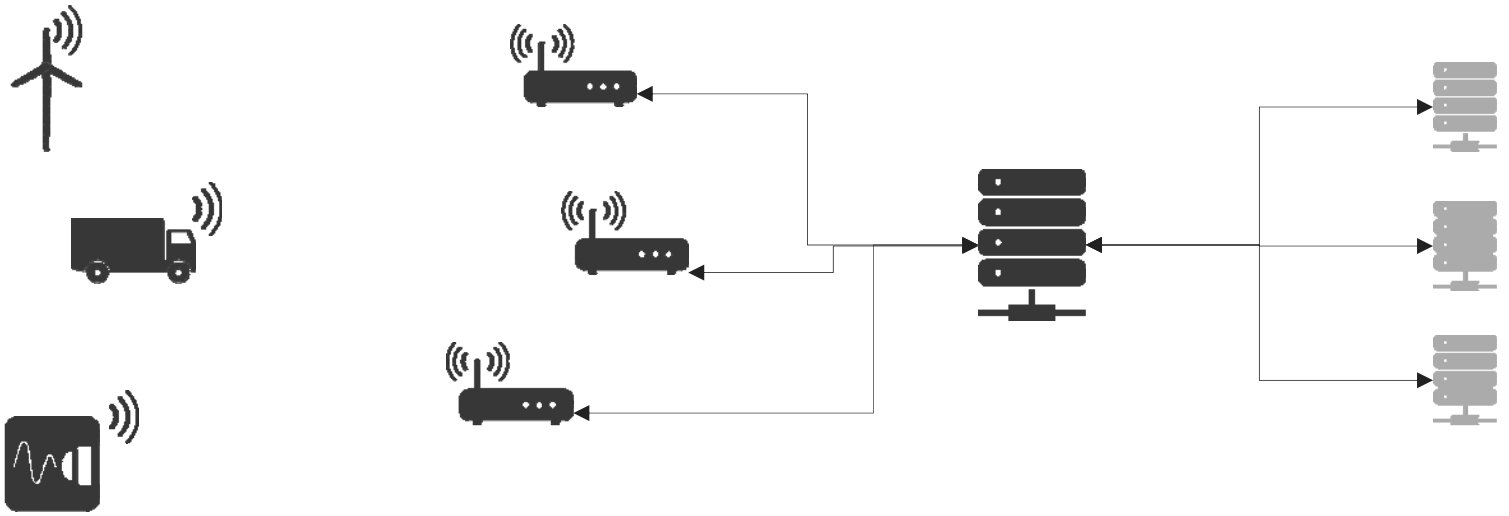
Requirements	WAN	LPWAN
Mutual auth.	 + AKA	Too costly Too much power
E2E sec.	  + TLS	Too costly Too much power

The LoRaWAN security example

LoRaWAN device (class A) communication



LoRa architecture



Devices

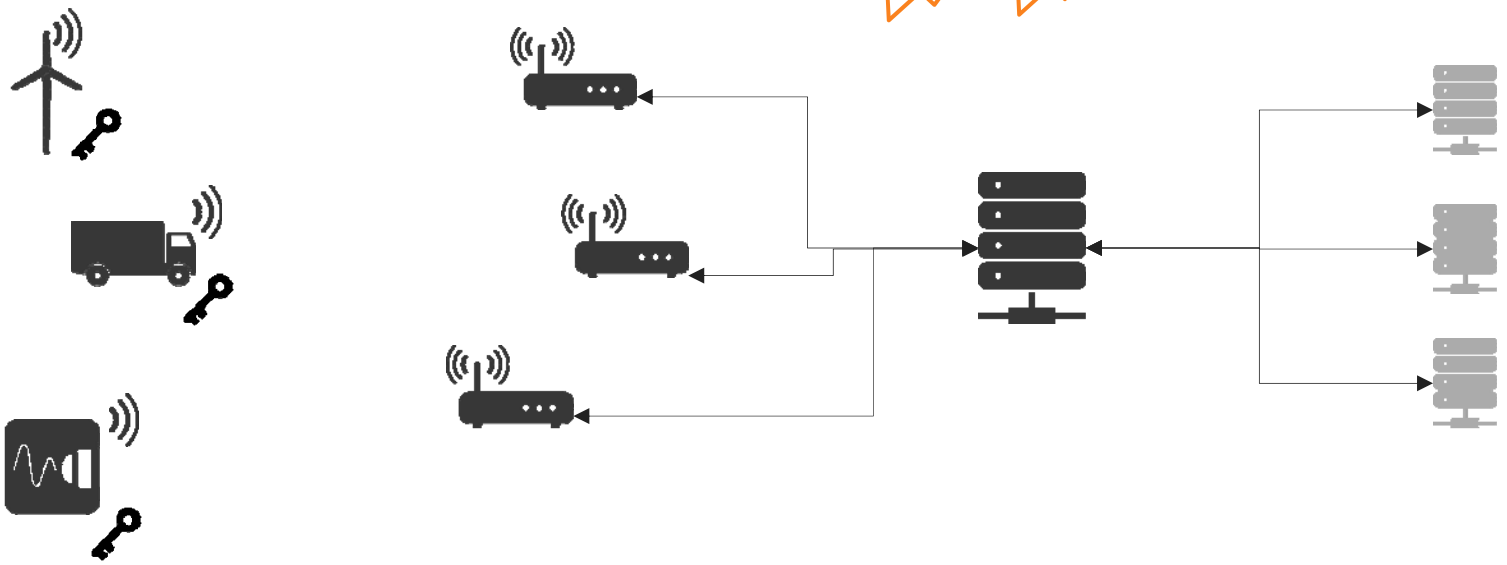
Gateways

LoRa network server

Application servers

LoRa security

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



Devices

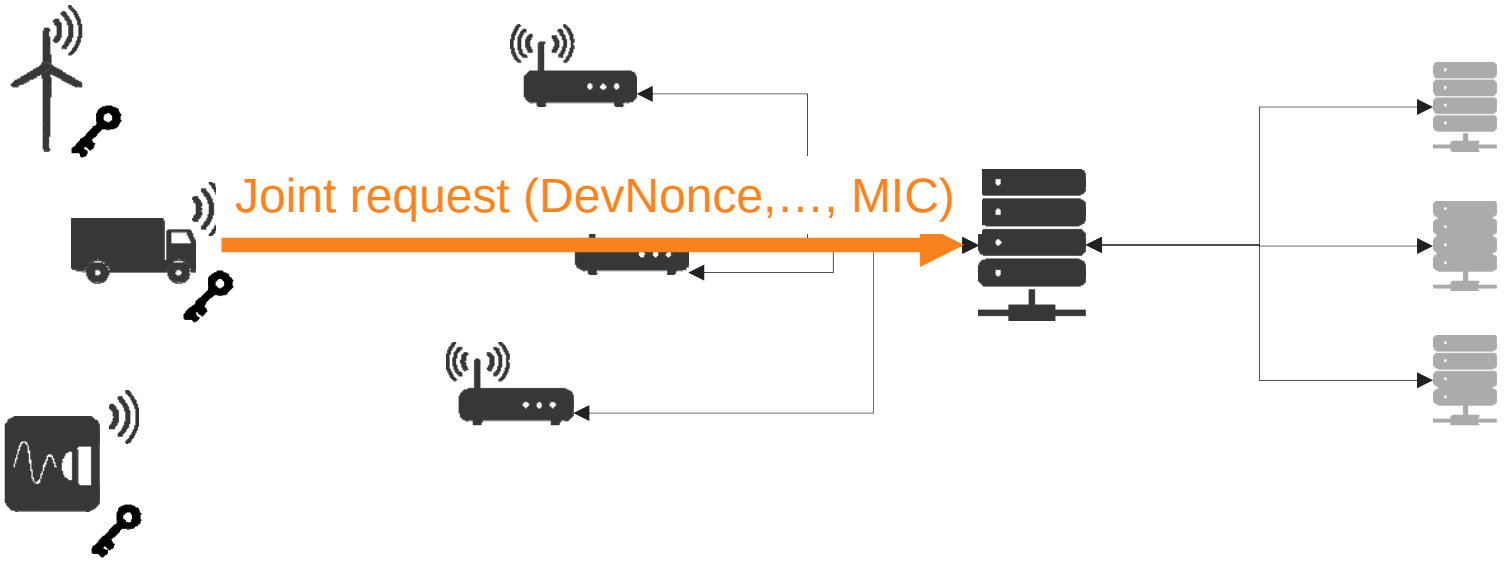
Gateways

LoRa network server

Application servers

LoRa security: network connection

A cryptogram (MIC) is computed with AppKey



Devices

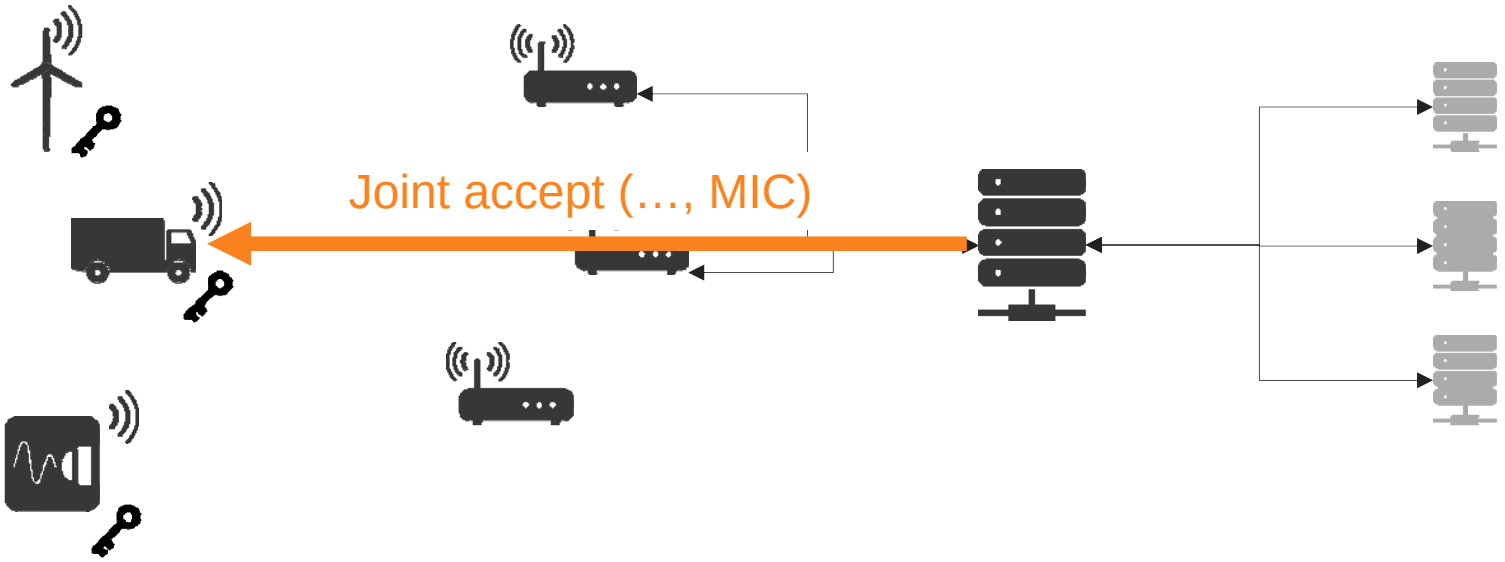
Gateways

LoRa network server

Application servers

LoRa security: network connection

A cryptogram (MIC) is also computed with AppKey



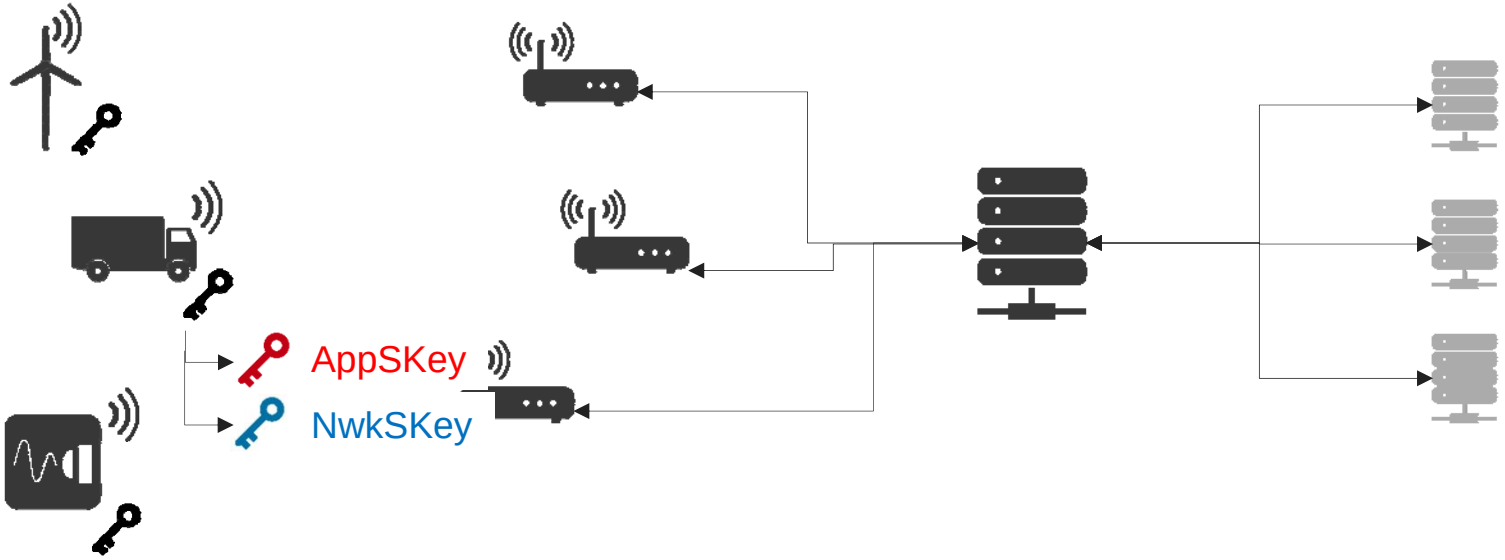
Devices | Gateways | LoRa network server | Application servers

Not a classic challenge / response scheme

- Saves a round trip
- But nonce is generated by the device to be authenticated
- Server-side has to check for replays

LoRa security: network connection

Two session keys are derived : AppSKey and NwkSKey



Devices

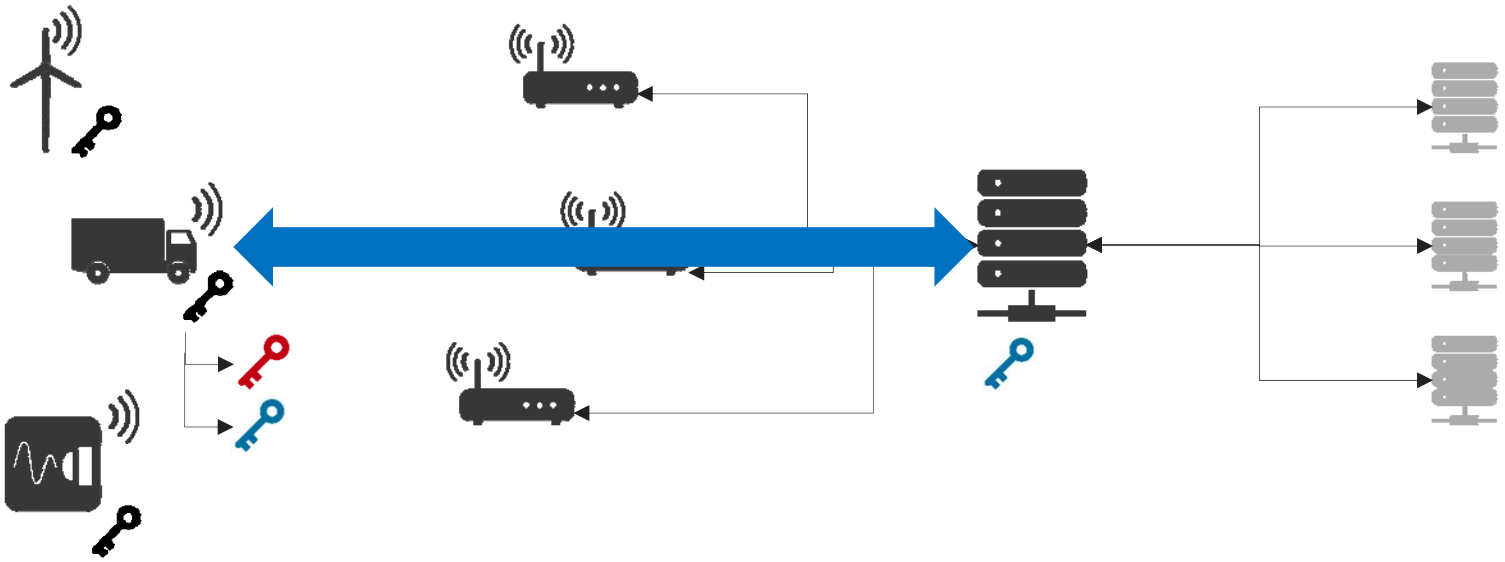
Gateways

LoRa network server

Application servers

LoRa security: network connection

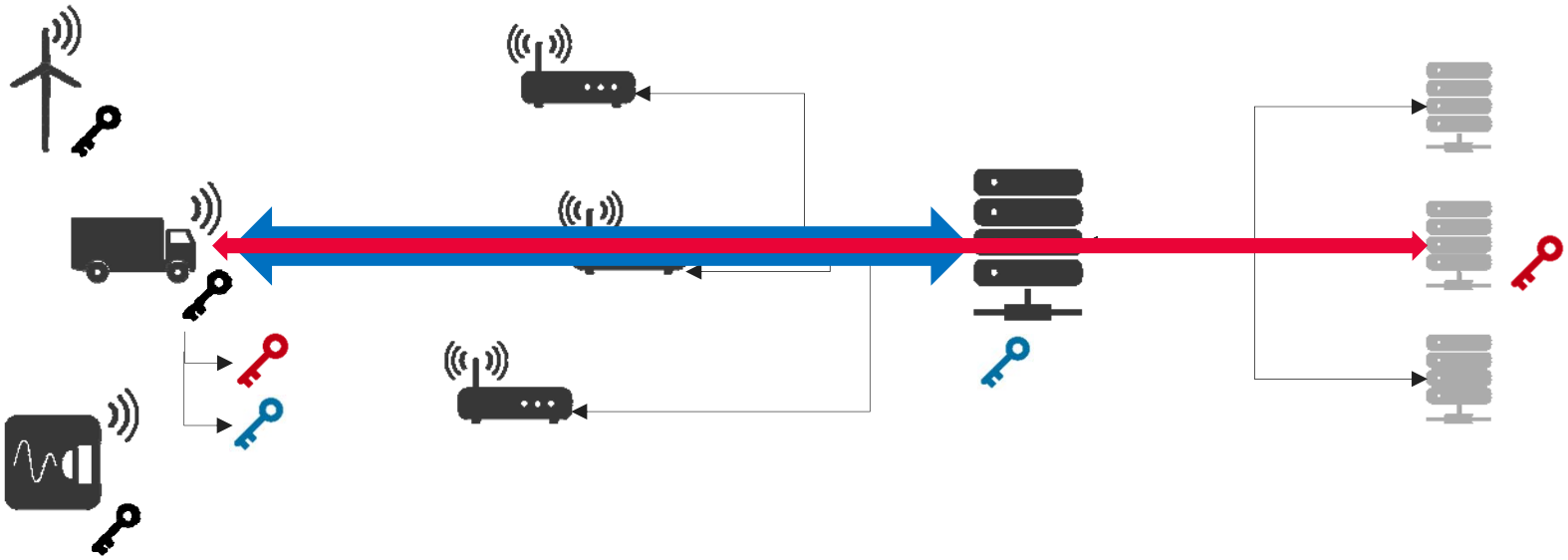
NwkSkey is used for network layer security



Devices | Gateways | LoRa network server | Application servers

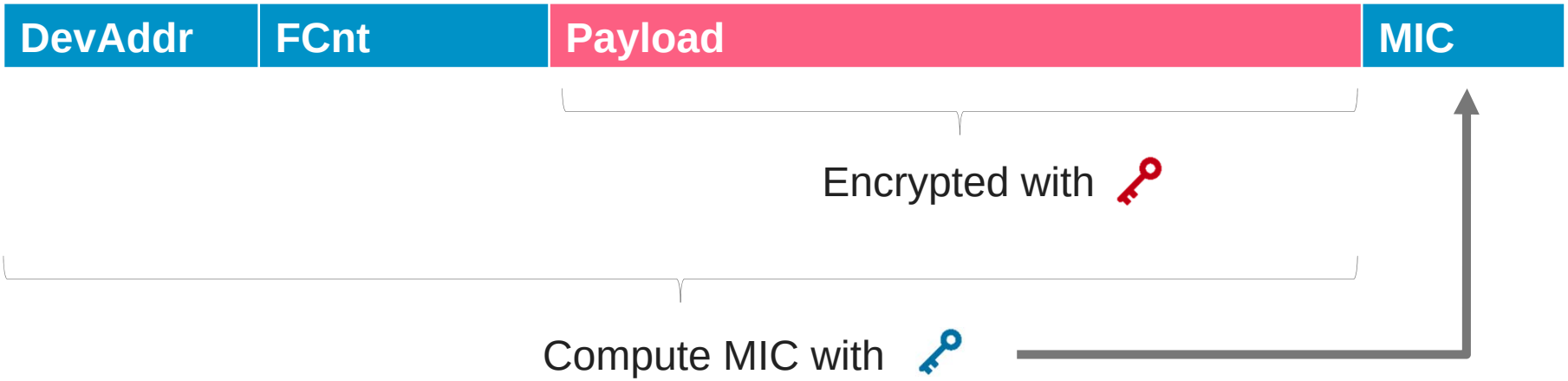
LoRa security: network connection

AppSkey is used for application layer end to end security



Devices | Gateways | LoRa network server | Application servers

LoRaWAN frame content for payloads



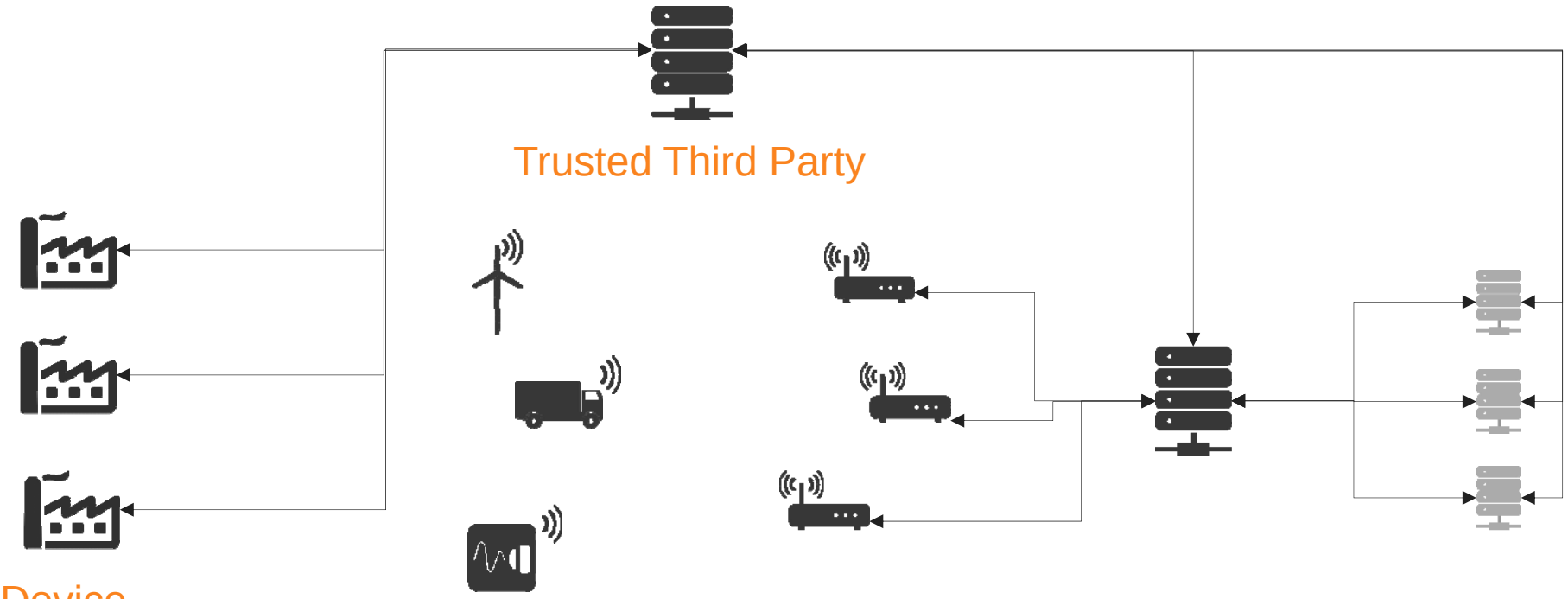
How to provision the keys ?

Problem statement for secure key provisioning

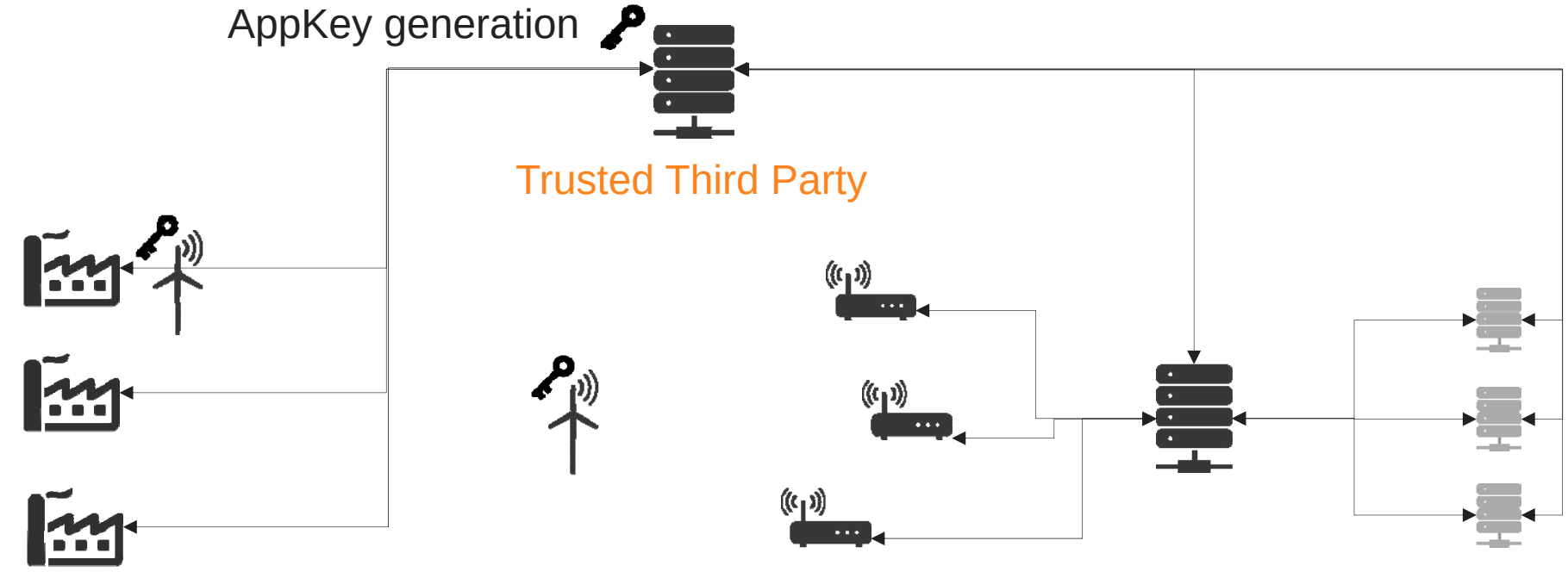
- How to provision the devices / servers without Secure Elements ?
- As the same key (AppKey) is used to derive both the network key (NwkSKey) and the applicative key (AppSkey), the network operator and its customers have a conflict of interest:
  - if the network operator knows the device key AppKey, it will be able to compute the AppSkey and thus intercept the applicative data;
  - if the application provider knows the device key AppKey, it will be able to compute the NwkSKey and thus clone devices.

- A Trusted Third party is needed !

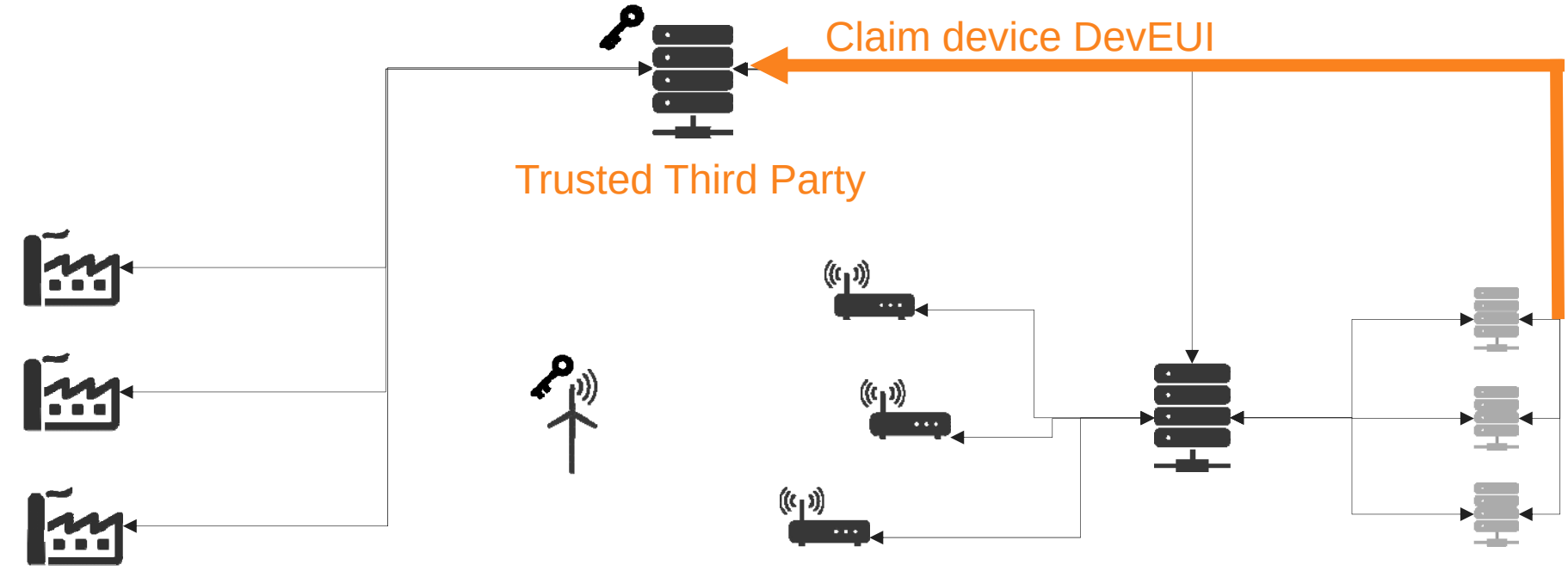
Introduction of a Trusted Third Party



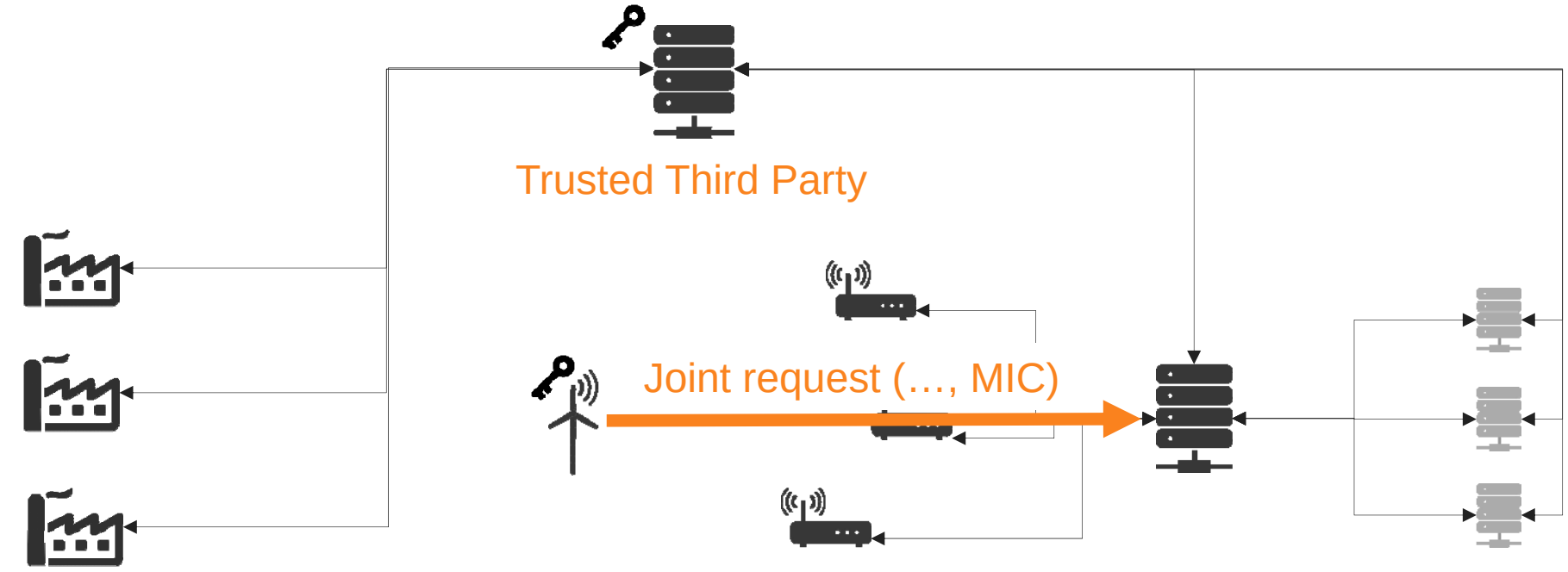
Device provisioning



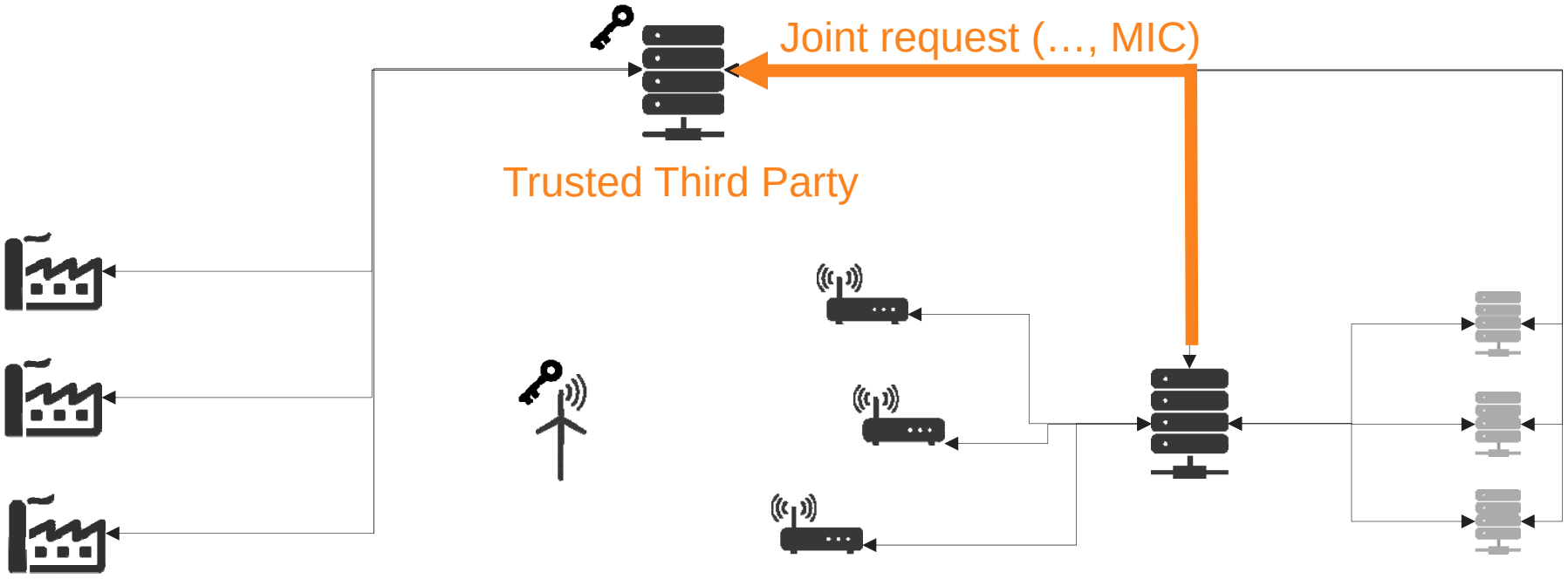
Device claiming



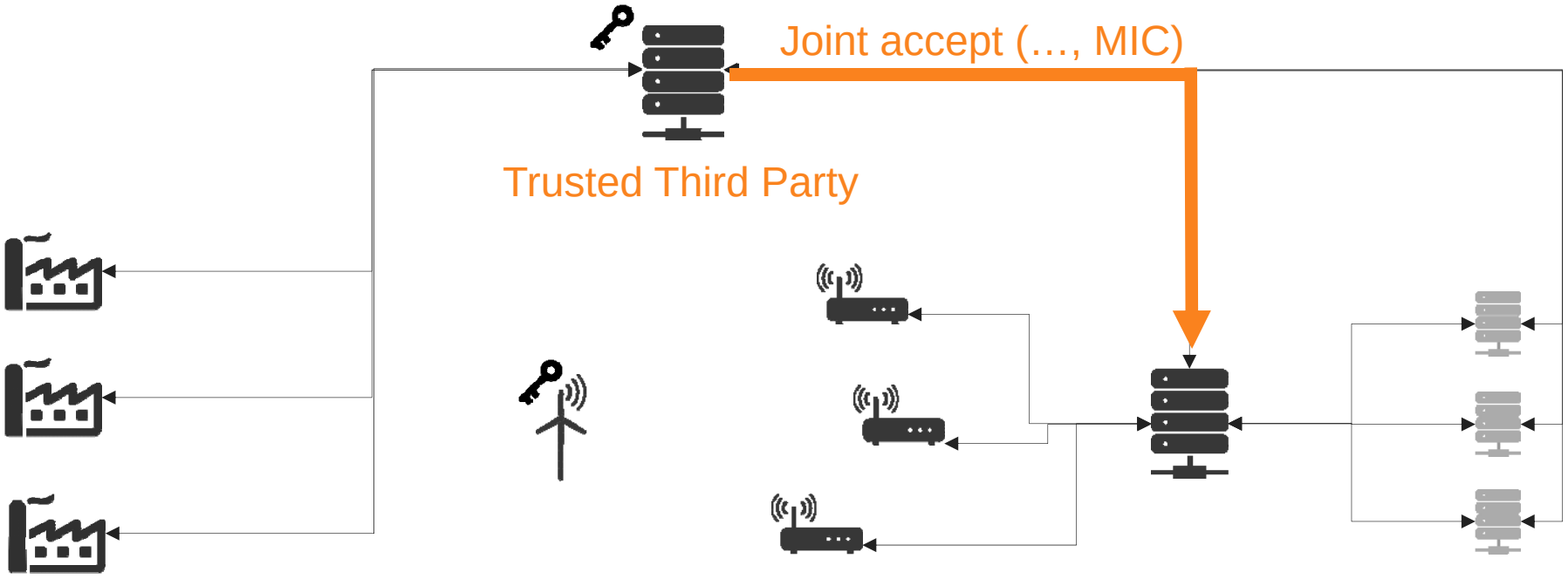
Network connection



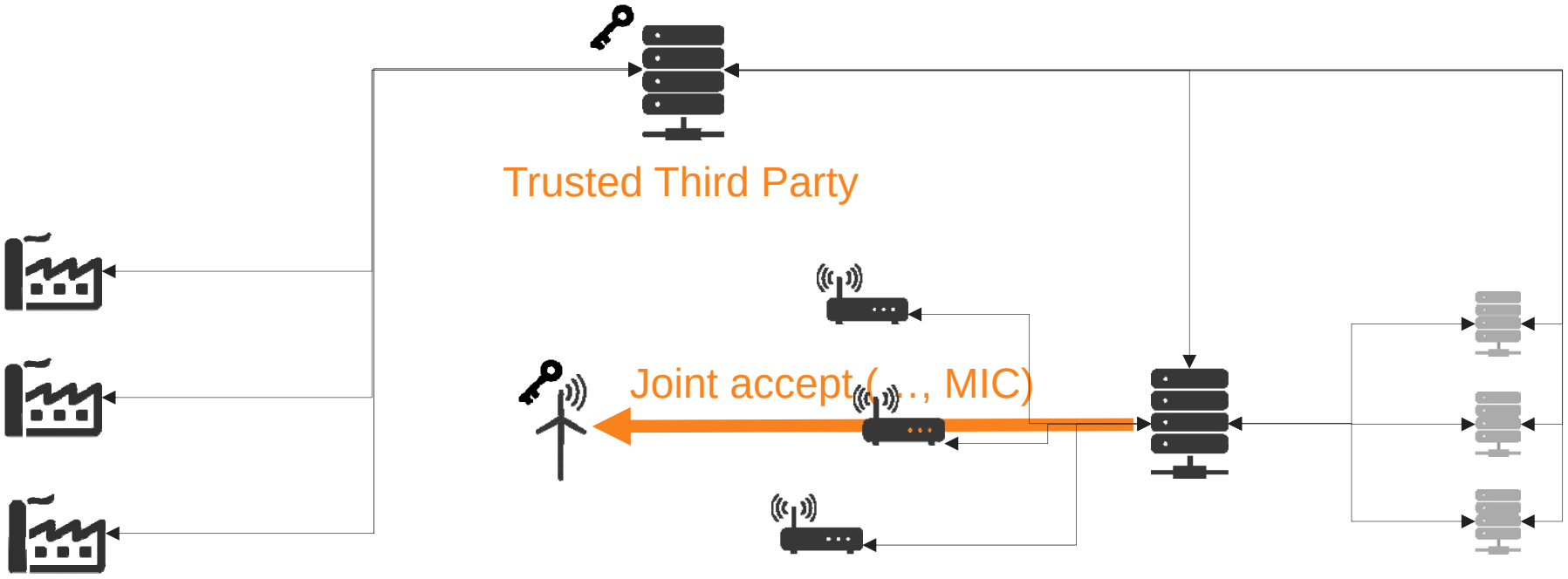
Network connection



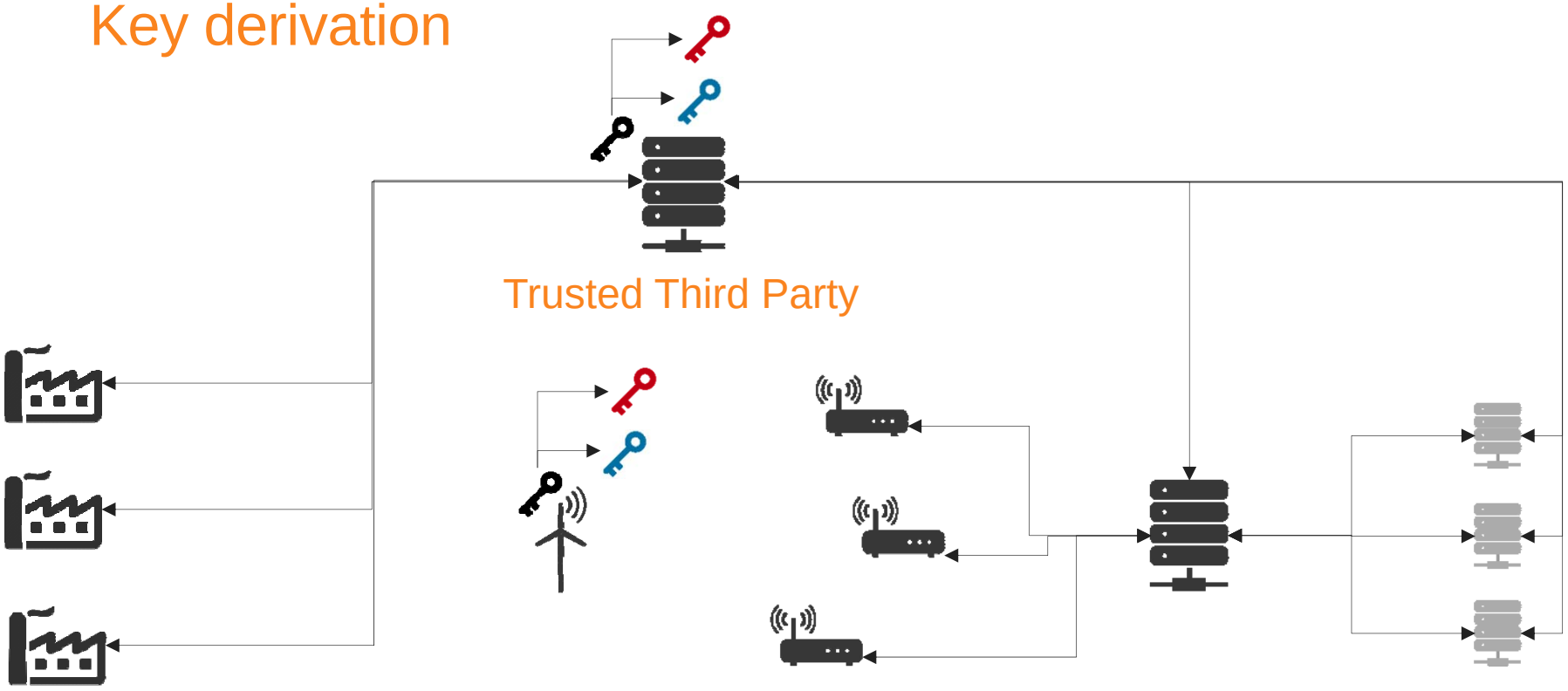
Network connection



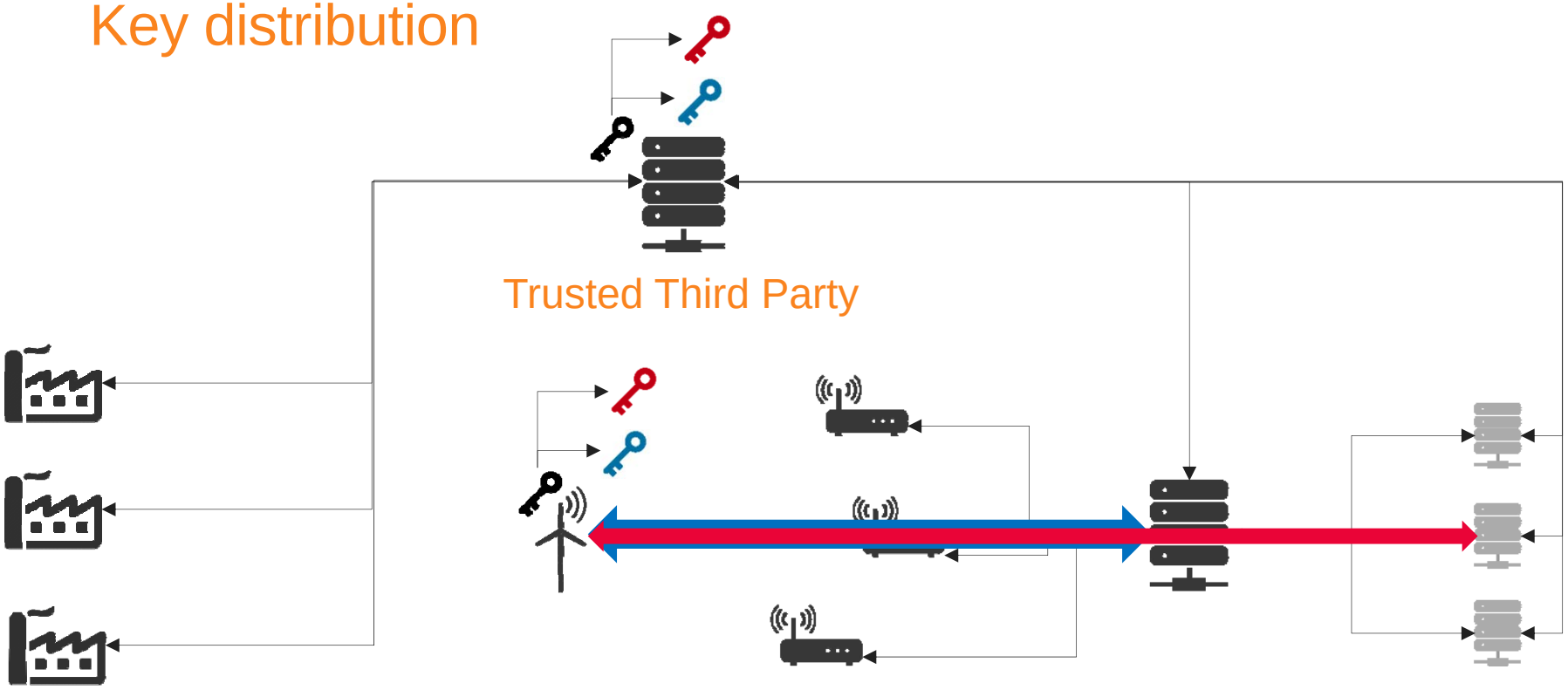
Network connection



Key derivation



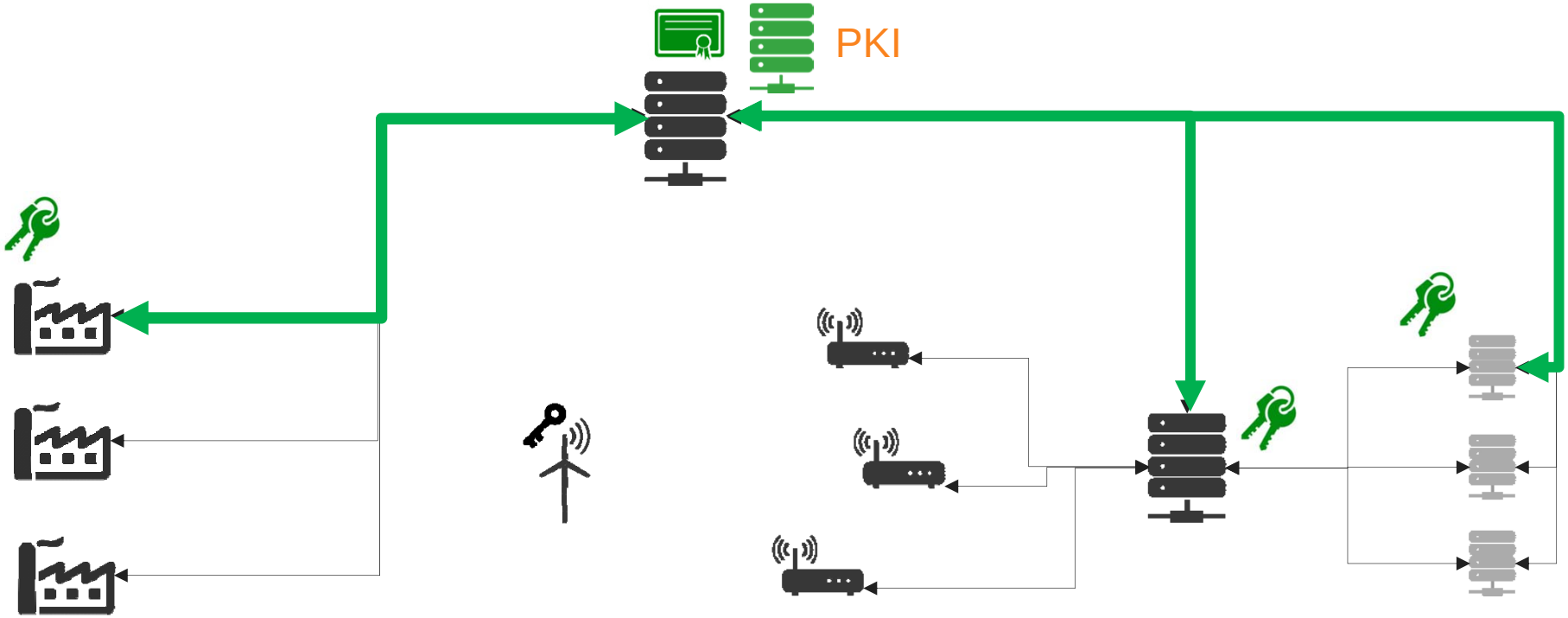
Key distribution



Trusted Third Party

Device manufacturers

Secure communication with TLS



Conclusion

- LPWAN drivers are low cost and low power
- Trust is needed, more than ever !
- A new trust infrastructure is required

Thanks for your attention