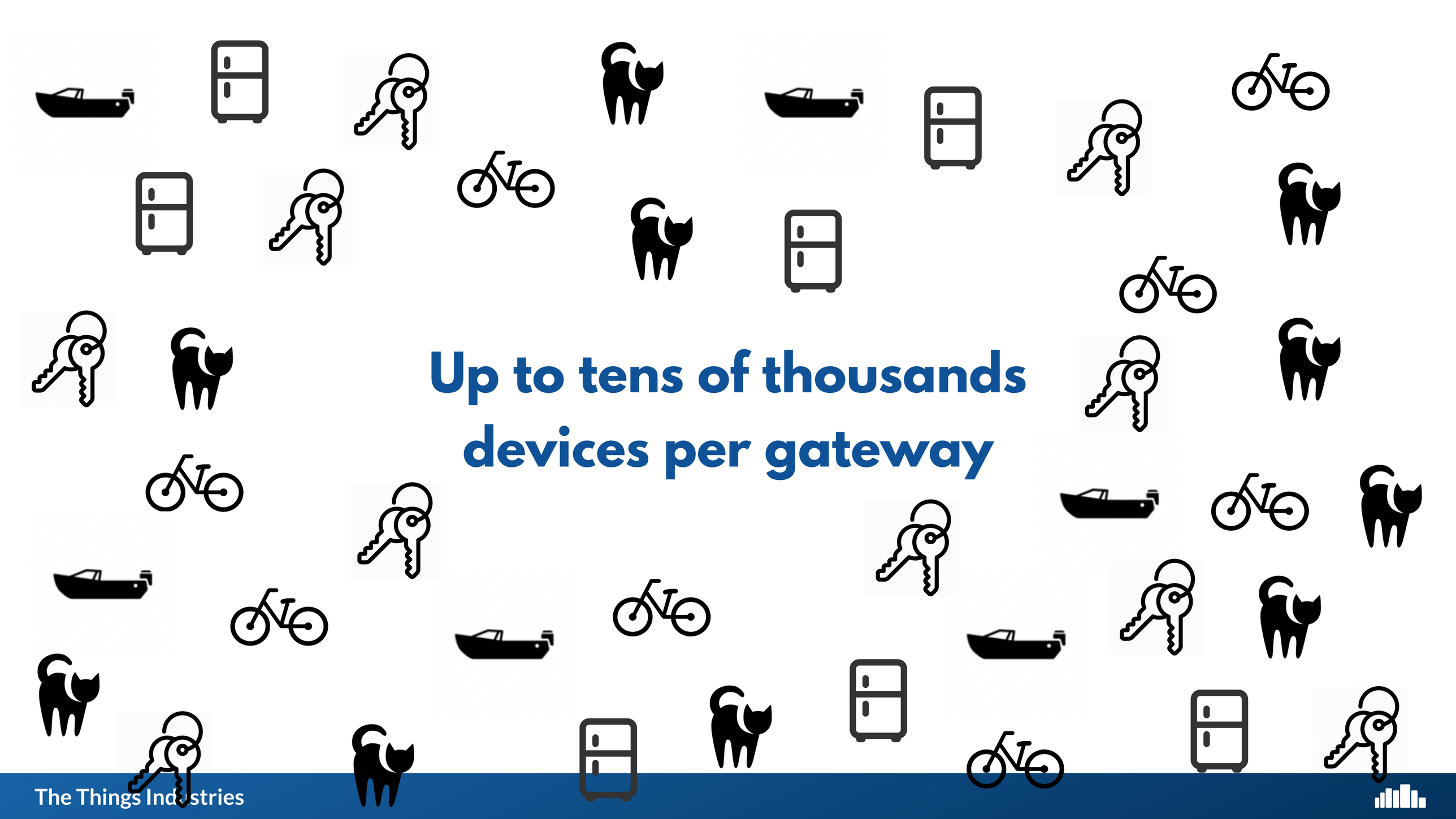
Introduction to LoRaWAN and Security Aspects

Johan Stokking
@johanstokking

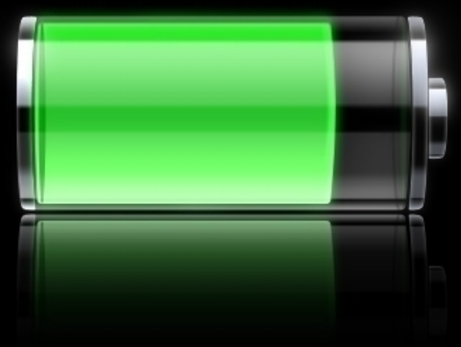
CTO and Co-Founder, The Things Industries
Tech Lead and Co-Founder, The Things Network
Chair, Security Working Group, LoRa Alliance


LoRaWAN™

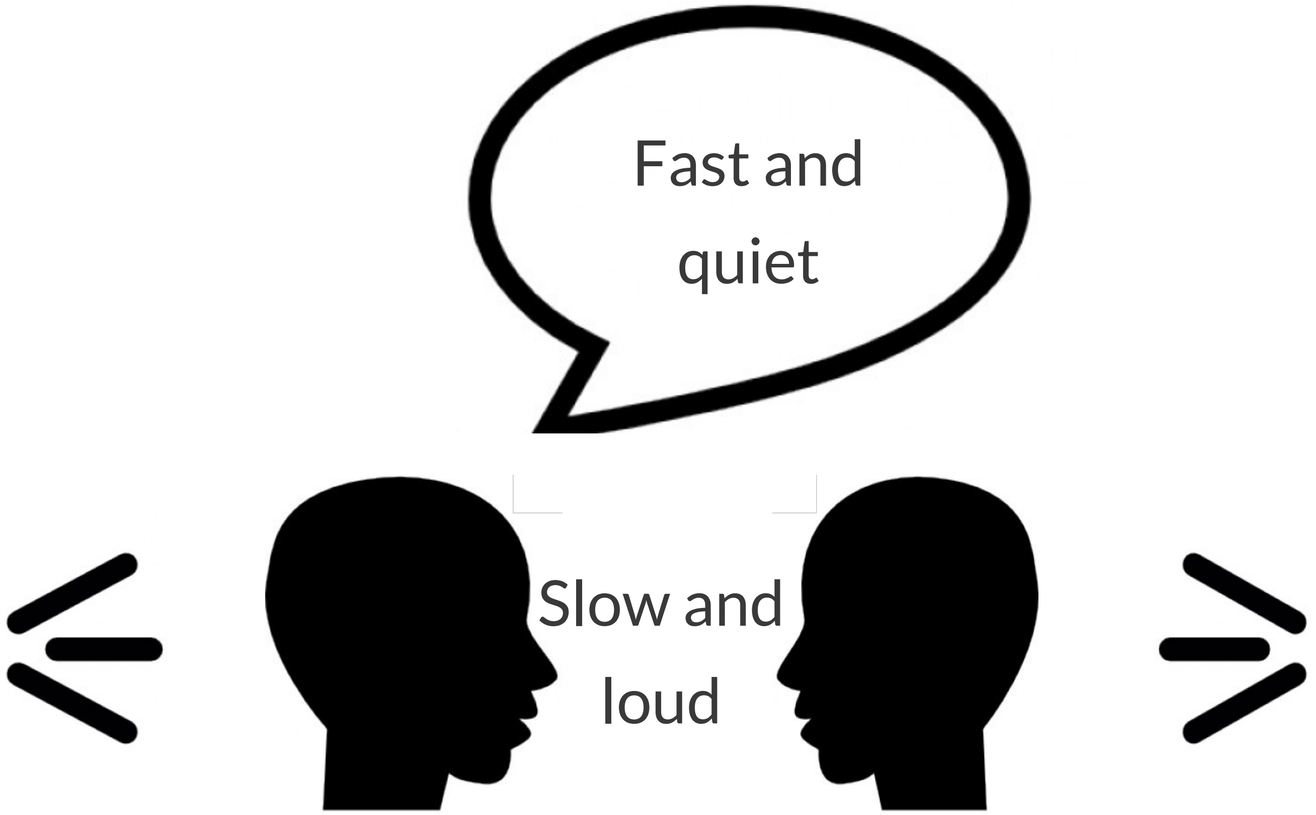


Up to tens of thousands devices per gateway

Low power and small messages

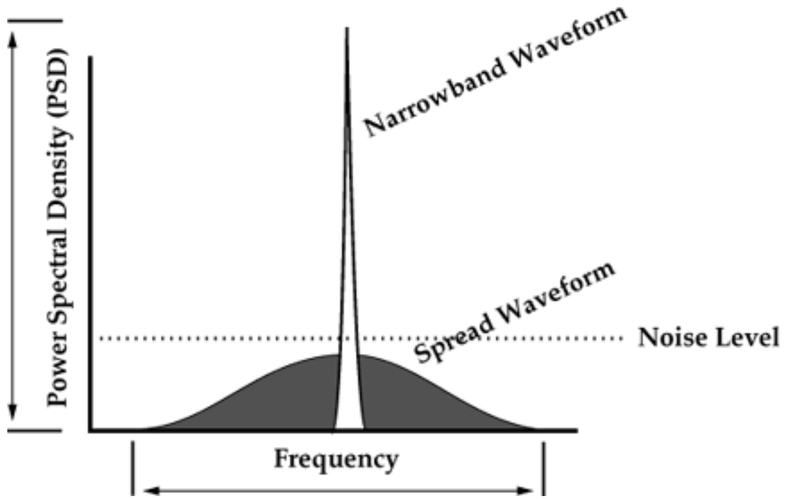


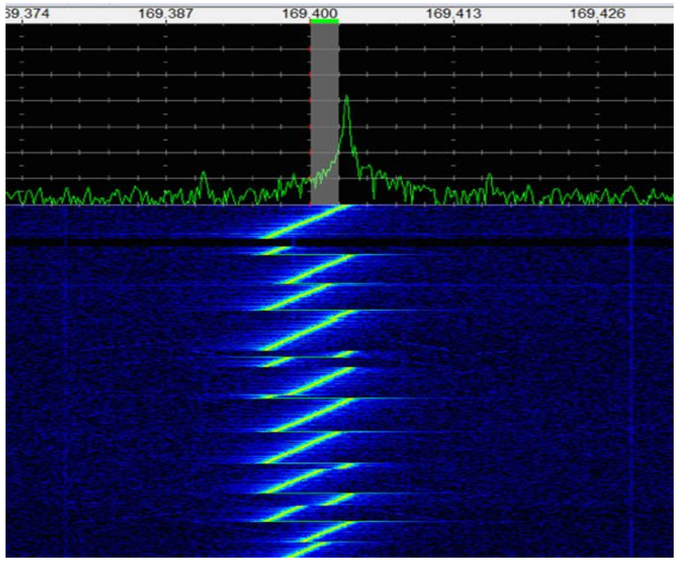
so devices can run on solar panels
for months or years on batteries


Fast and
quiet
Slow and
loud

LoRa: modulation for wireless transmission

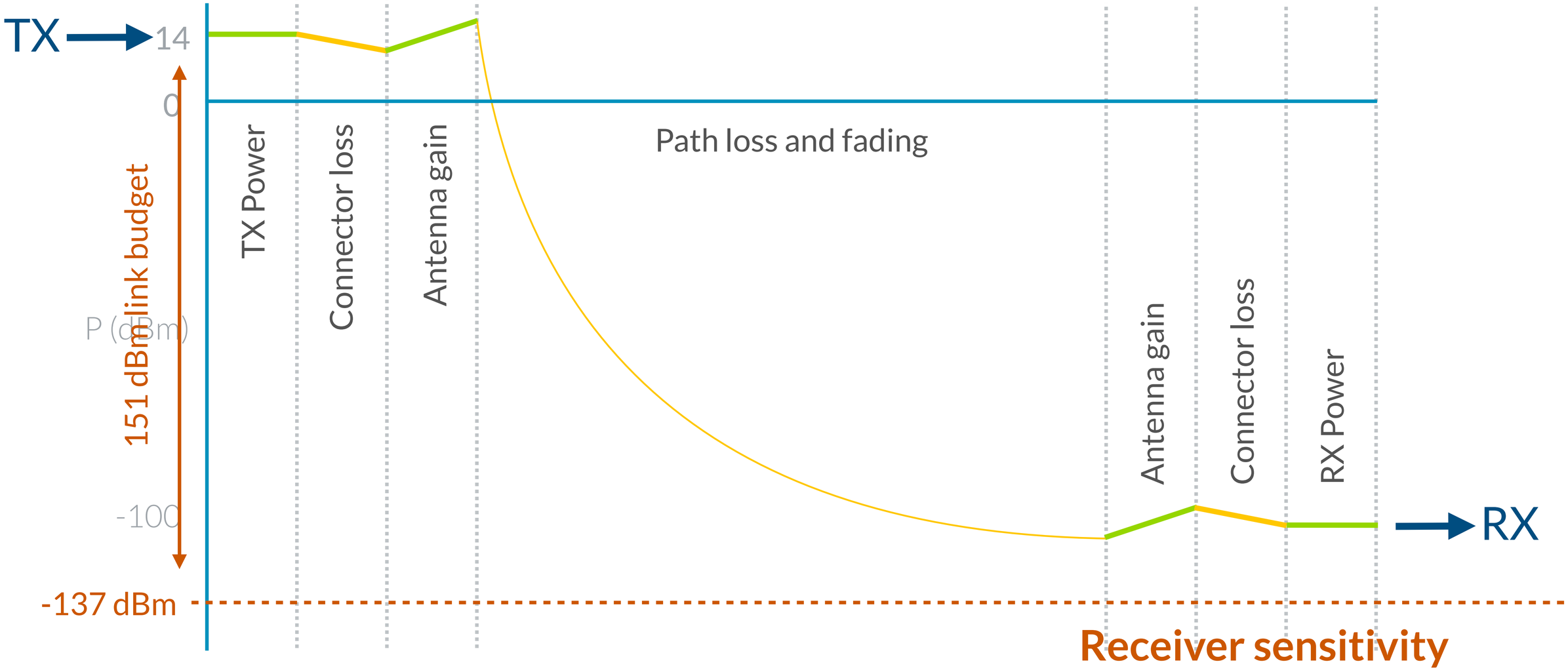
Spread-spectrum; robust to interference, multi-path and fading





40 BBAA0126 80 D204 2A A50EDB DB2A5FFA

LoRa wireless performance



LoRa wireless performance

	TX Power	RX Sensitivity	Link budget
Wi-Fi	20.5 dBm	-75 dBm	**95.5 dBm**
LoRa	14 dBm	-137 dBm	**151 dBm**
NB-IoT	23 dBm **x 8**	-129 dBm	**152 dBm**

$$FSPL = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) - G_t - G_r$$

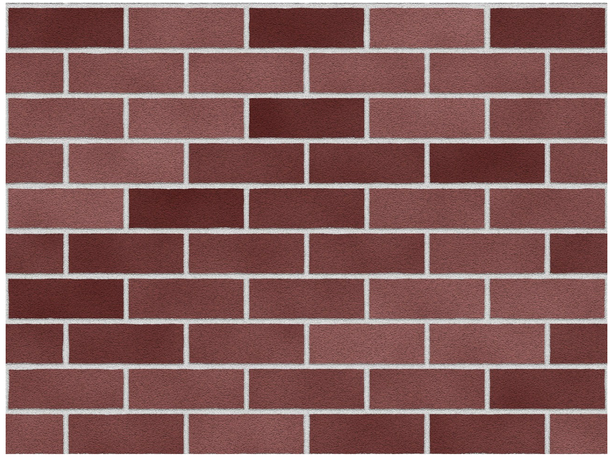
LoRa wireless performance

Theoretical maximum in free space is **850 km** (US915 regulations)

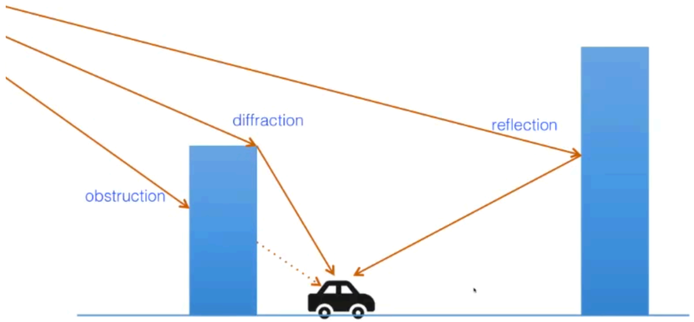
Wi-Fi is only **550 meters**

The Things Network Community set the world record: **832 km** using a helium balloon

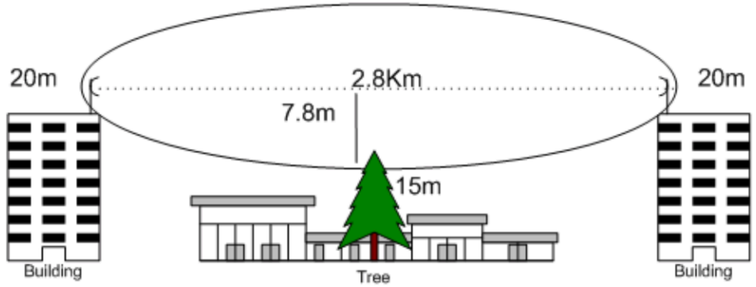
Free space is only in space



Attenuation



Reflection and diffraction



Fresnel zone

Complementary to:

Differentiators and benefits

Public and private deployment options

Firmware updates over the air

Geolocation

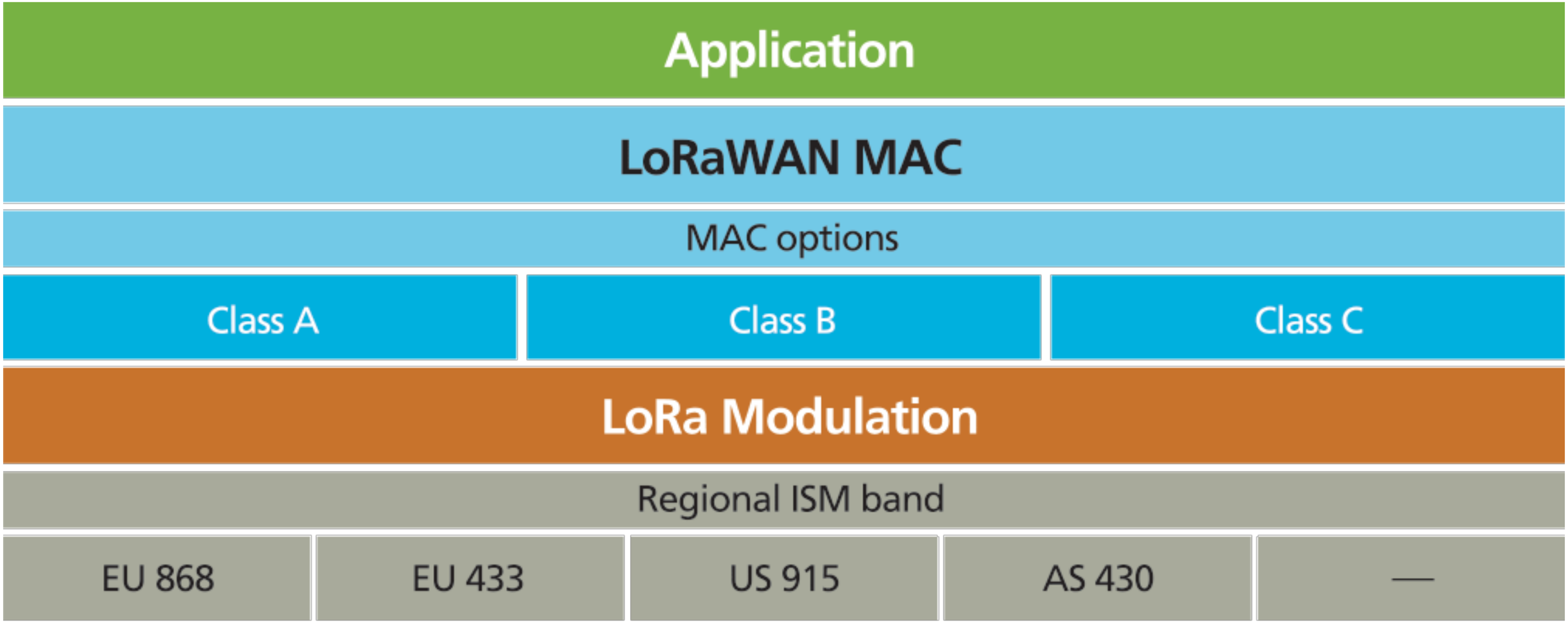
End-to-end security

Supports 10+ years battery lifetime

Long range

Deep indoor penetration

LoRa and LoRaWAN



Open, crowd sourced and decentralized community network

Largest global LoRaWAN network

142
Countries

900
Cities

11150
Gateways

106K
Developers

11M
Packets/day

Empower with tools

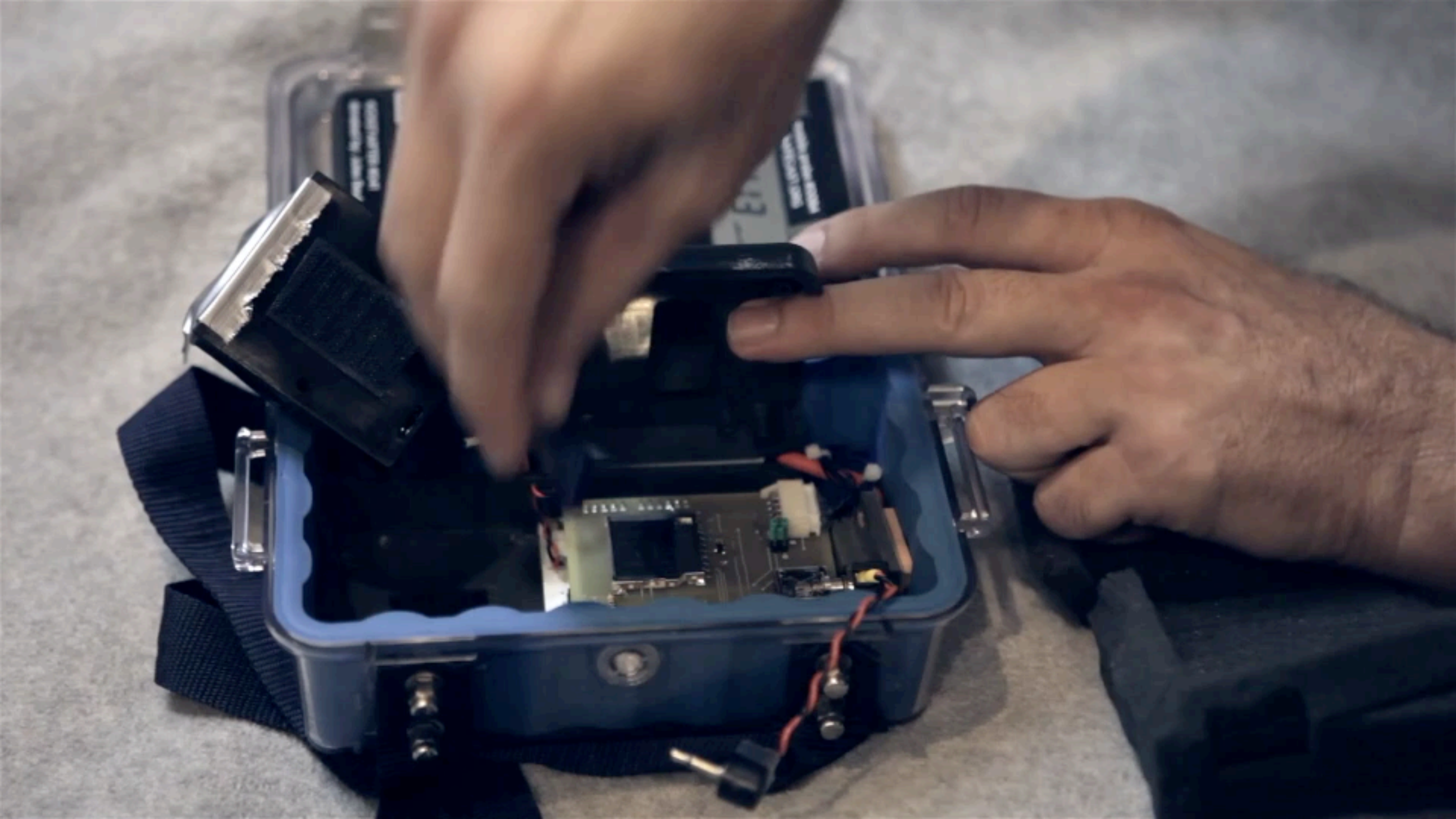
ENTERPRISE

THE THINGS STACK


Rabobank
SODAQ

irnas

THE THINGS NETWORK




U
DB
15
S5
Strausberg Nord
S9
S7
Schönefeld
Ahrensfelde
2 min
7 min
482 417-3


DB

The Things Enterprise Stack

Best in class LoRaWAN Network Server

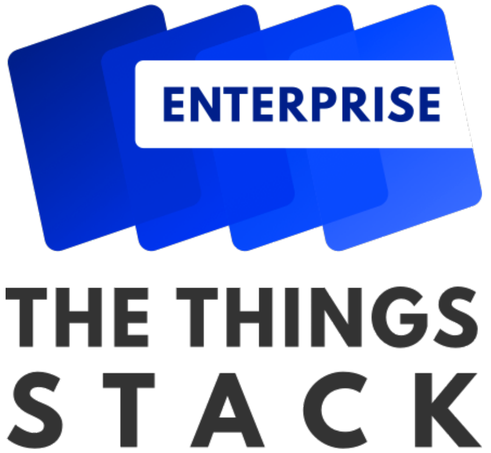
Built from scratch for scale, security, global distribution

API first design and loosely coupled components

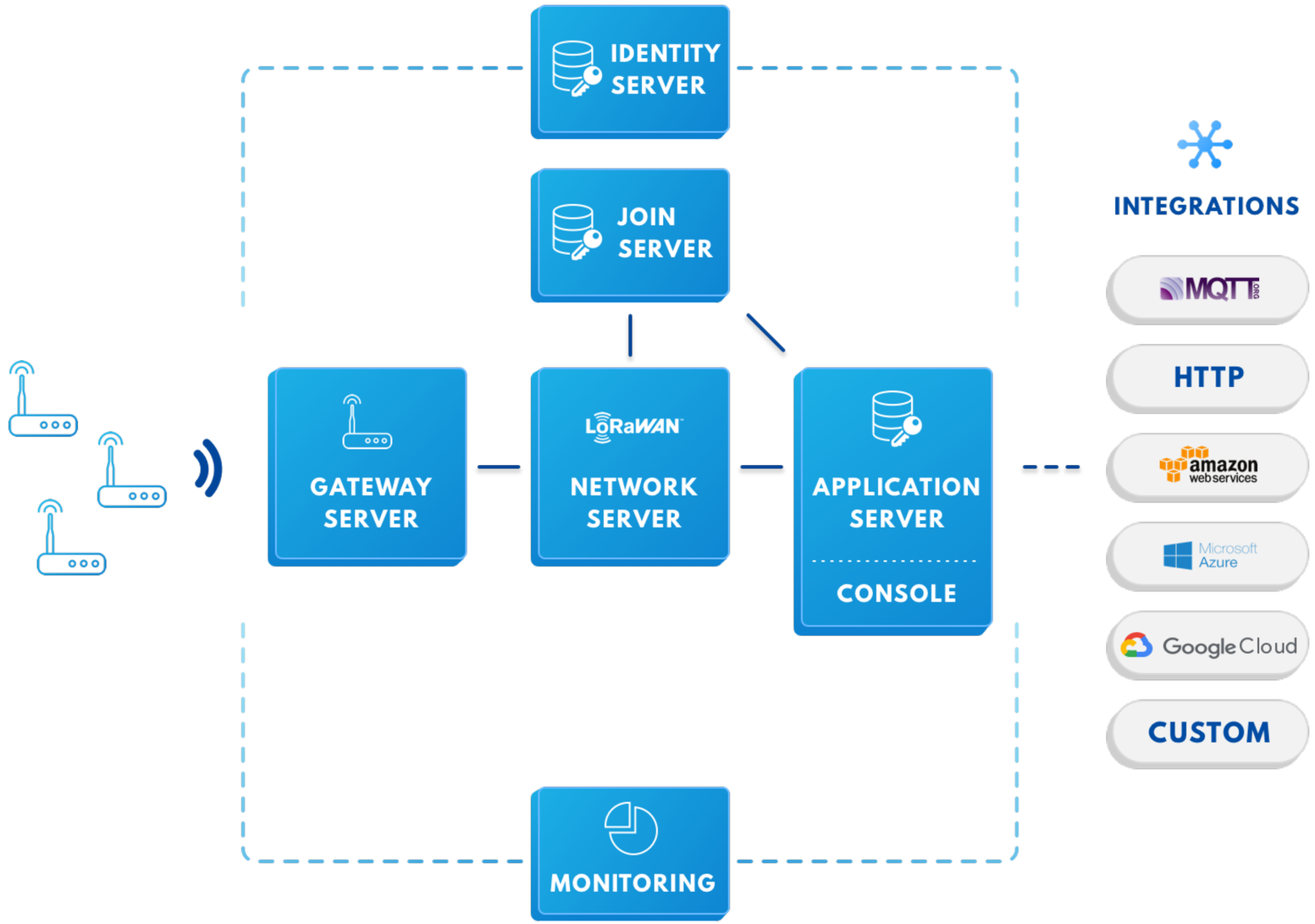
Powered by the open source The Things Stack

Commercially available in four distributions

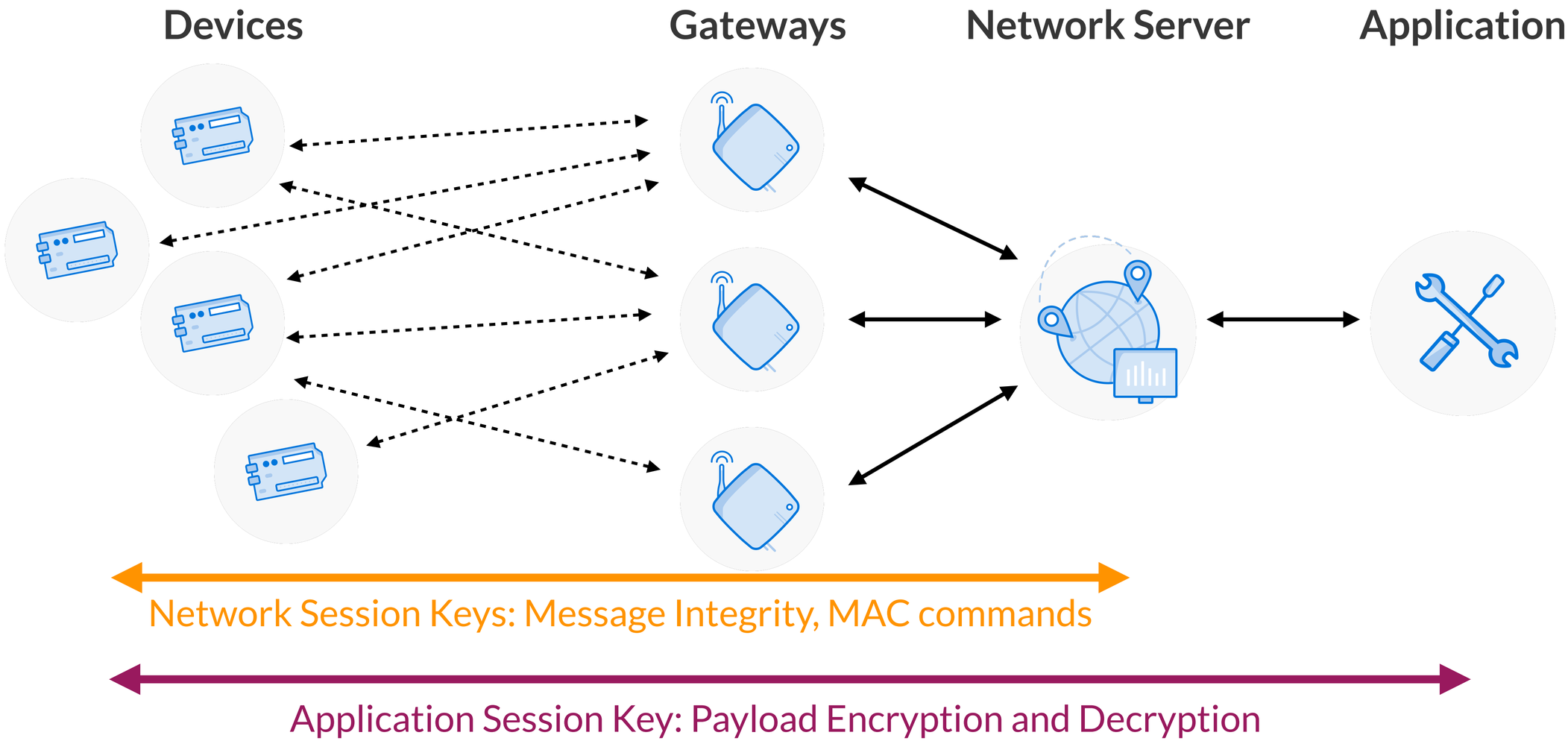
Supports peering across all deployment models



The Things Enterprise Stack



LoRaWAN network topology



Symmetric Cryptographic Security Primitives

Threats	Protecting Tools	Security primitives and procedures
Unauthorized access	Mutual end point authentication	Join procedure: AES128 – CMAC AES128 – ECB Electronic CodeBook
Modification	Integrity protection	MIC Message Integrity Check • AES128 – CMAC Cypher-based message authentication code • Device address is part of MIC • Frame Counter is part of MIC
Spoofing	Data origin authentication	
	Replay protection	
Eavesdropping	Encryption	AES128 – CTR Counter Mode Encryption

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

LoRaWAN session key derivation

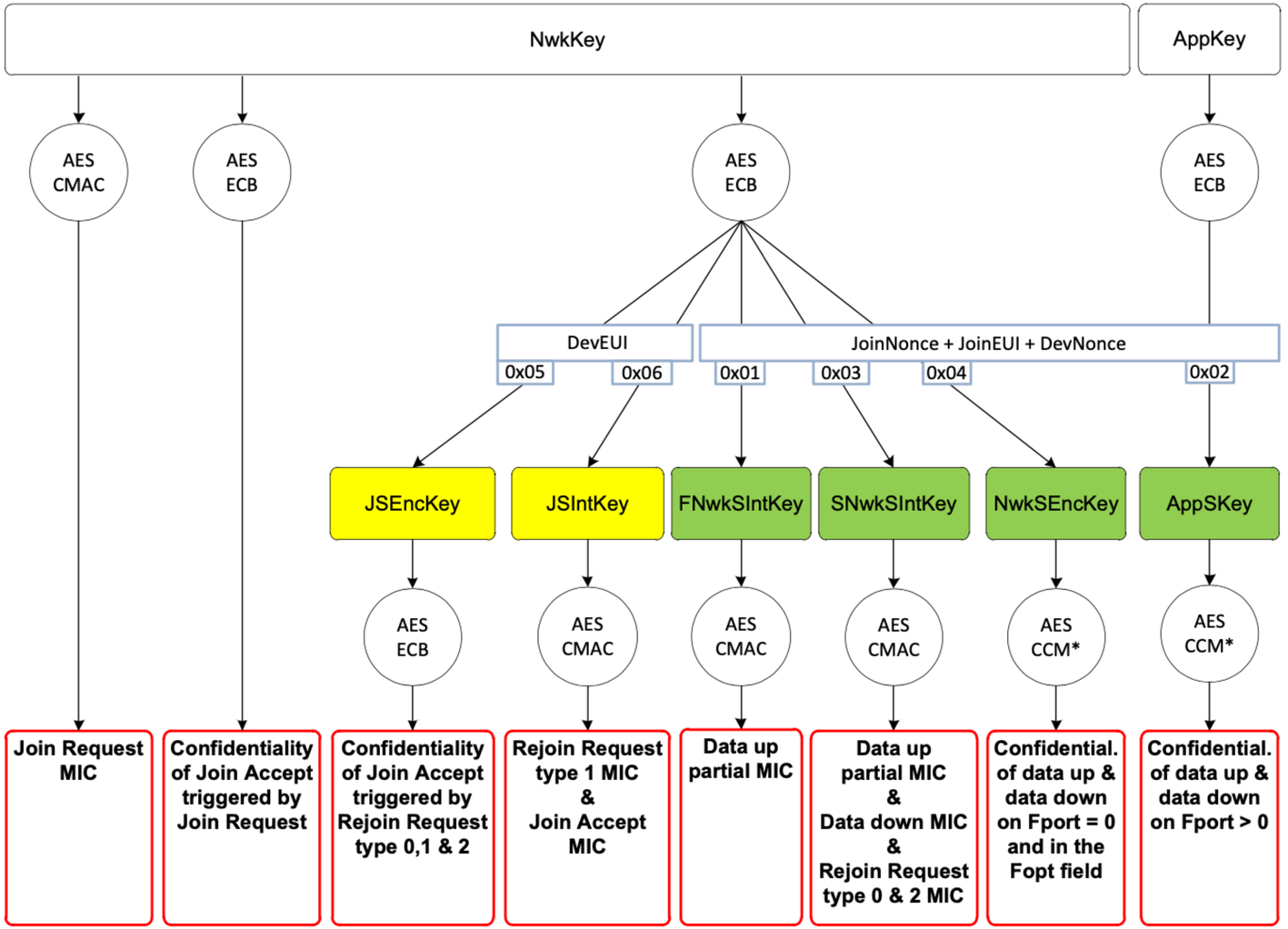
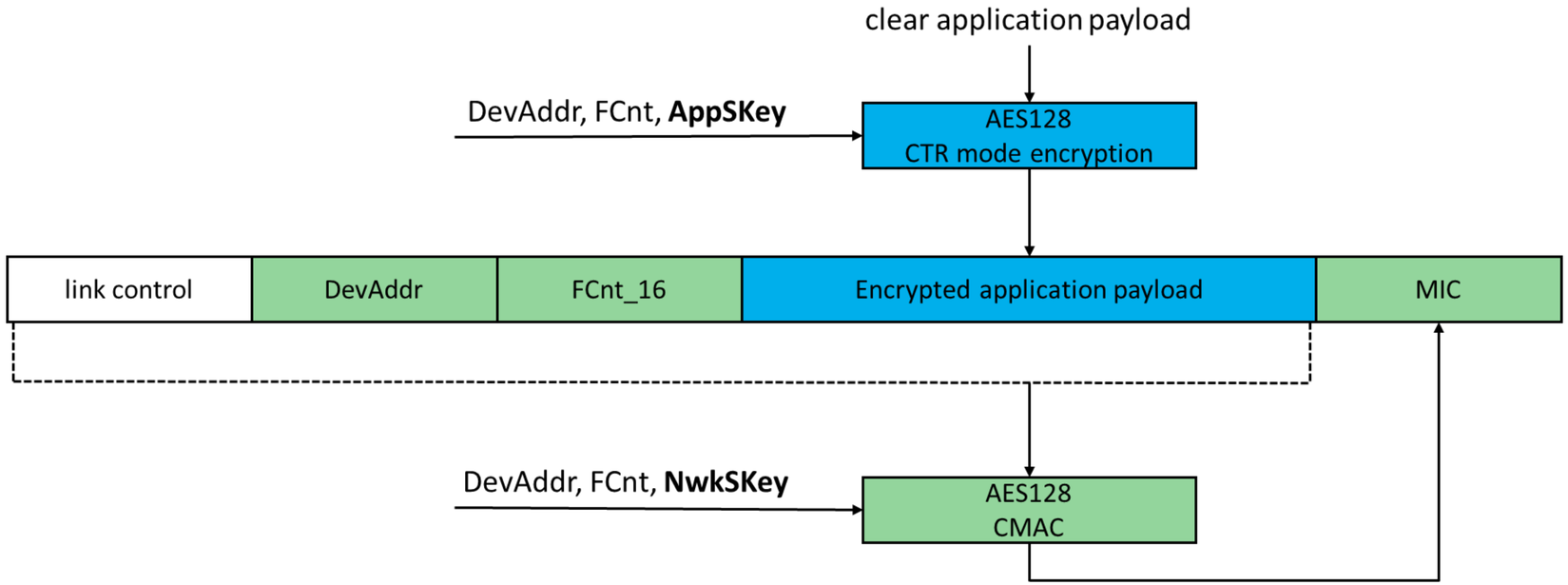


Figure 49 : LoRaWAN1.1 key derivation scheme

Frame Authentication and Encryption



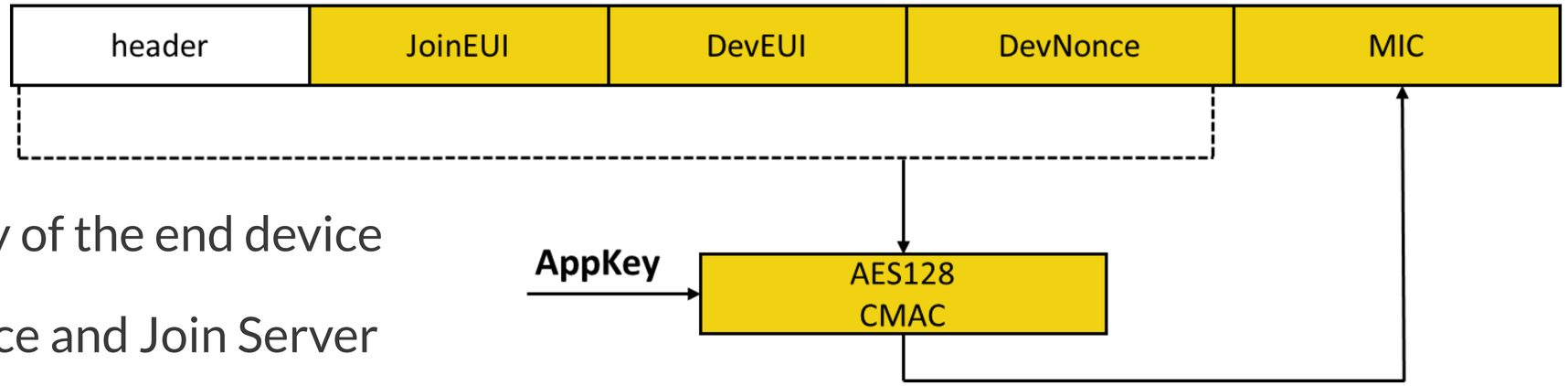
Message Integrity Check is 32 bits and can only be computed/verified with NwkSKey

Application Session Key (AppSKey) and Network Session Key (NwkSKey) are 128 bits

- They are specific to a device, which is identified by its address (DevAddr)
- They are renewed at each session, starting with device activation

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Joining a Network: Over The Air Activation (OTAA)



AppKey is the 128 bit root key of the end device

- Shared between end device and Join Server
- Unique, random, difficult to guess

DevEUI identifies the device

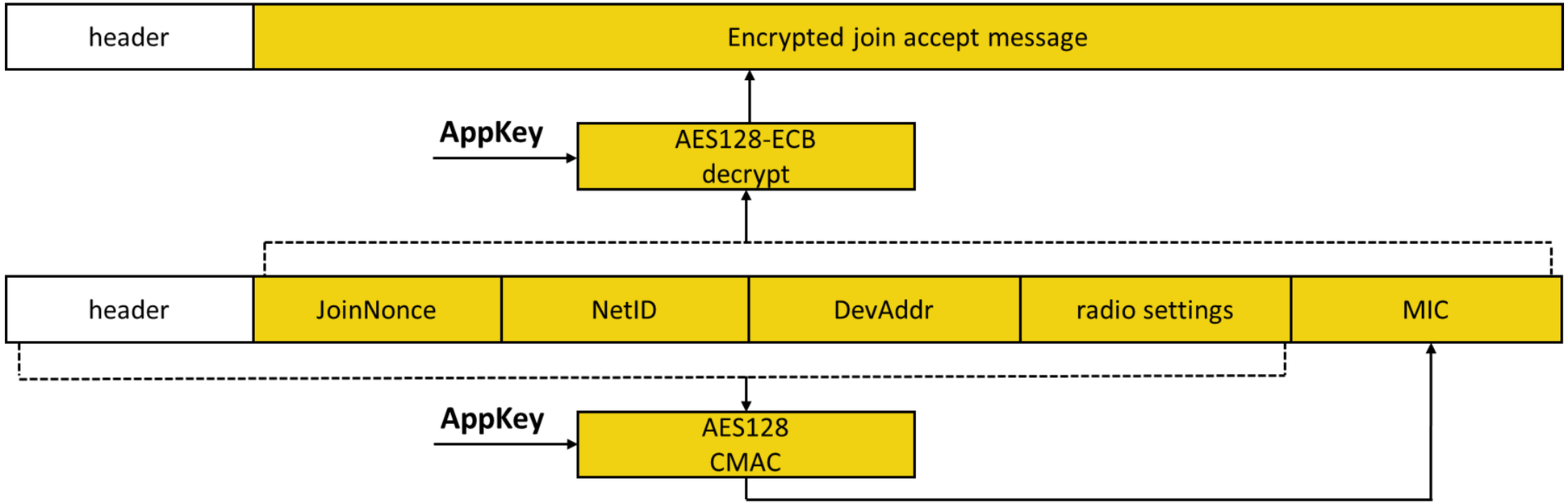
JoinEUI identifies the Join Server that knows (DevEUI, AppKey)

DevEUI and JoinEUI are EUI-64-based identifiers, allocated by IEEE

DevNonce is a counter to prevent replay attacks

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Joining a Network: Over The Air Activation (OTAA)



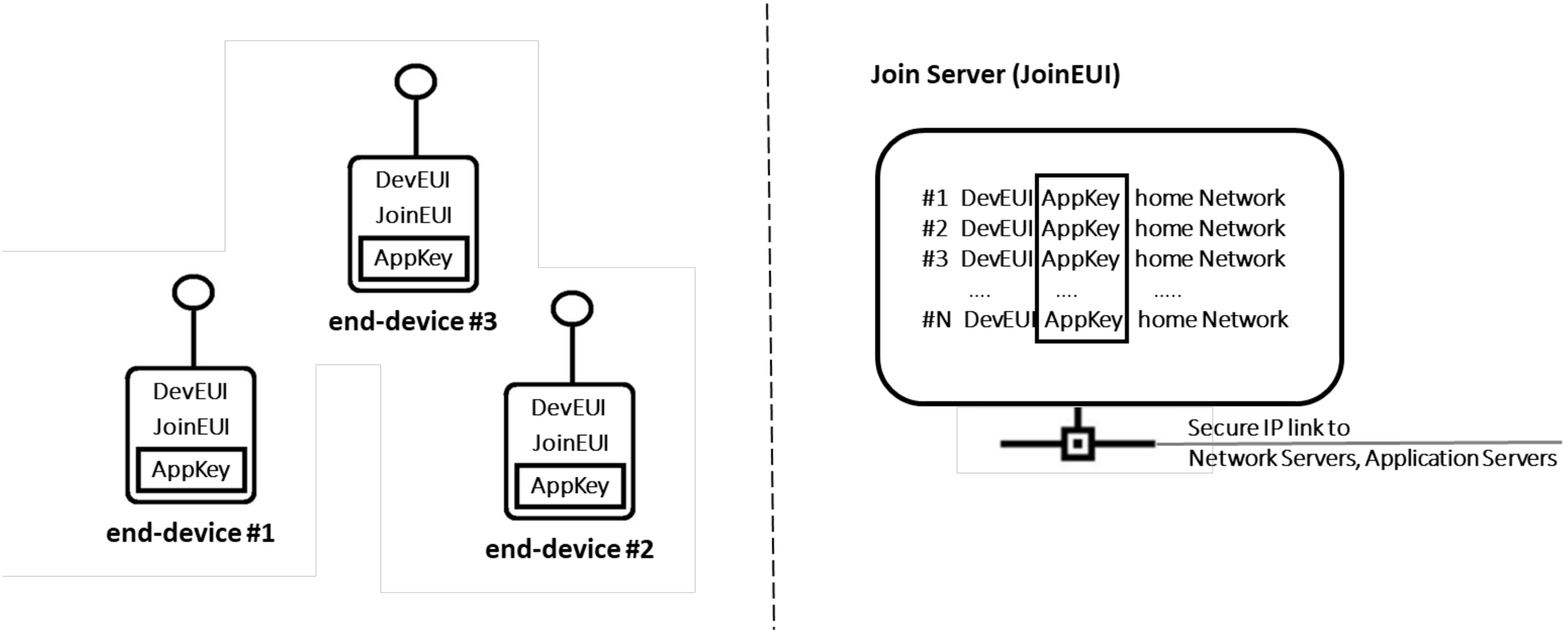
Only end device, which knows the AppKey, can decrypt the Join Accept frame and verify integrity

NwkSKey and AppSKey are derived using AES 128 encryption of AppKey, NetID, JoinNonce, DevNonce

The first uplink that follows Join Accept frame confirms the new session keys

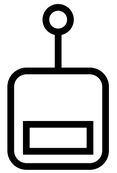
Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Device Provisioning

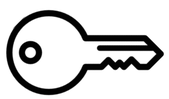


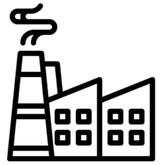
Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters



End Device





Device Manufacturer

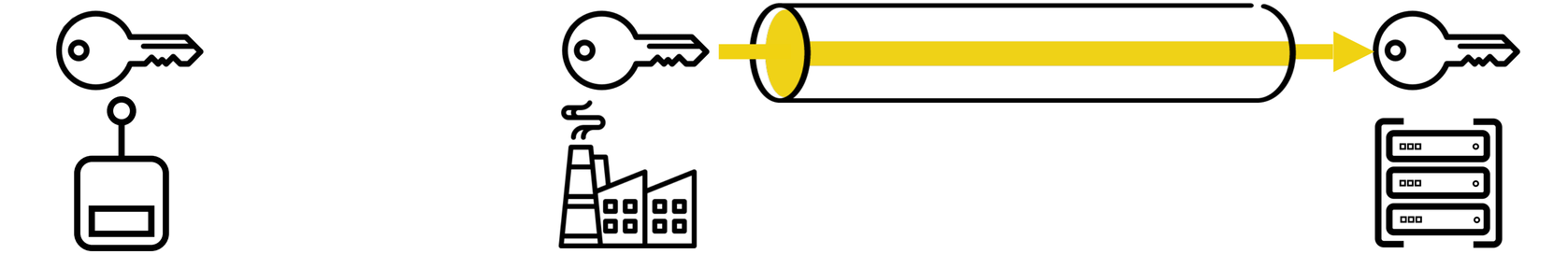
Root key (AppKey) generation

Unique per device

Strong (hard to guess)

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters

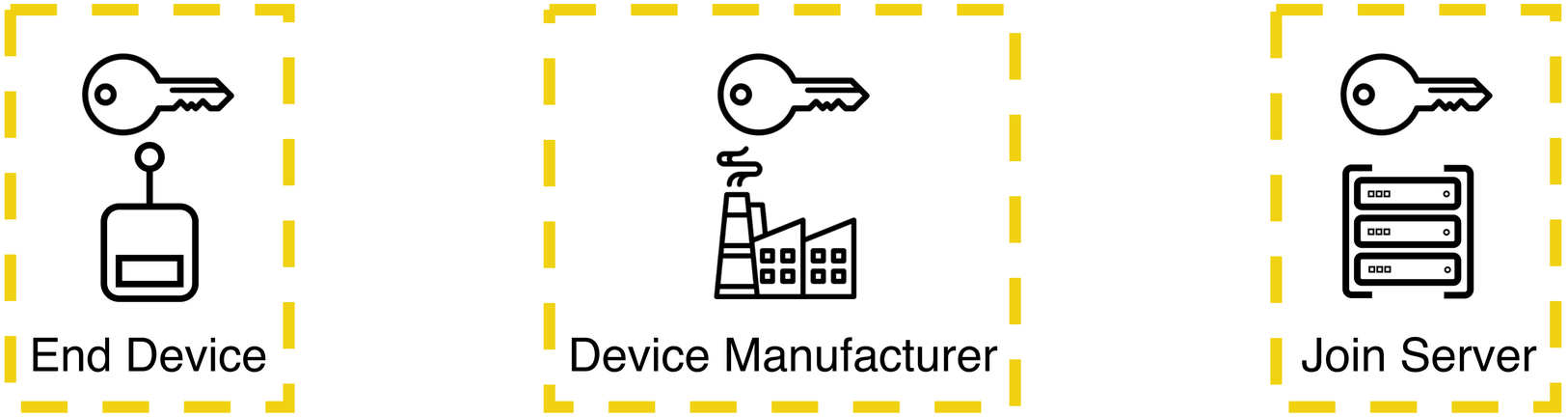


Root key delivery

End-to-end integrity protection and privacy

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters

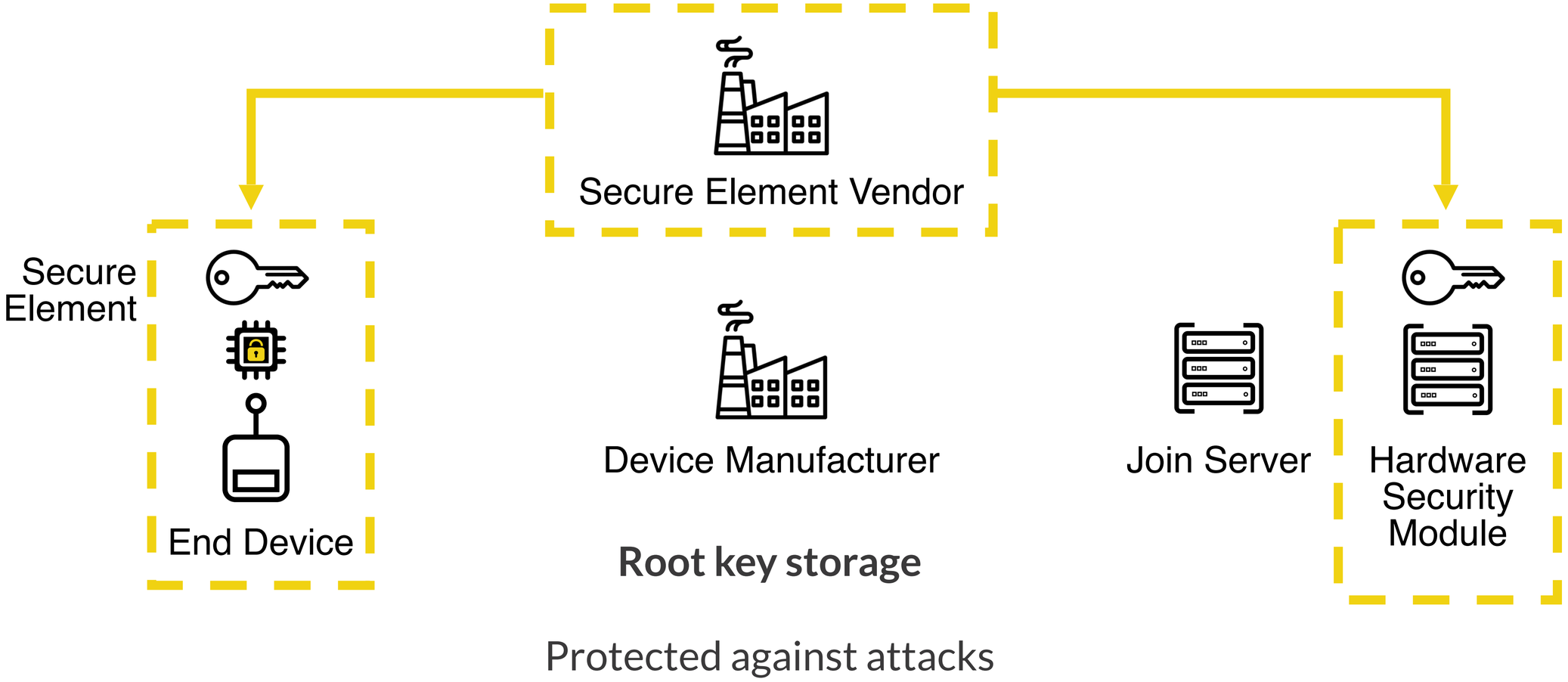


Root key storage

Protected against attacks

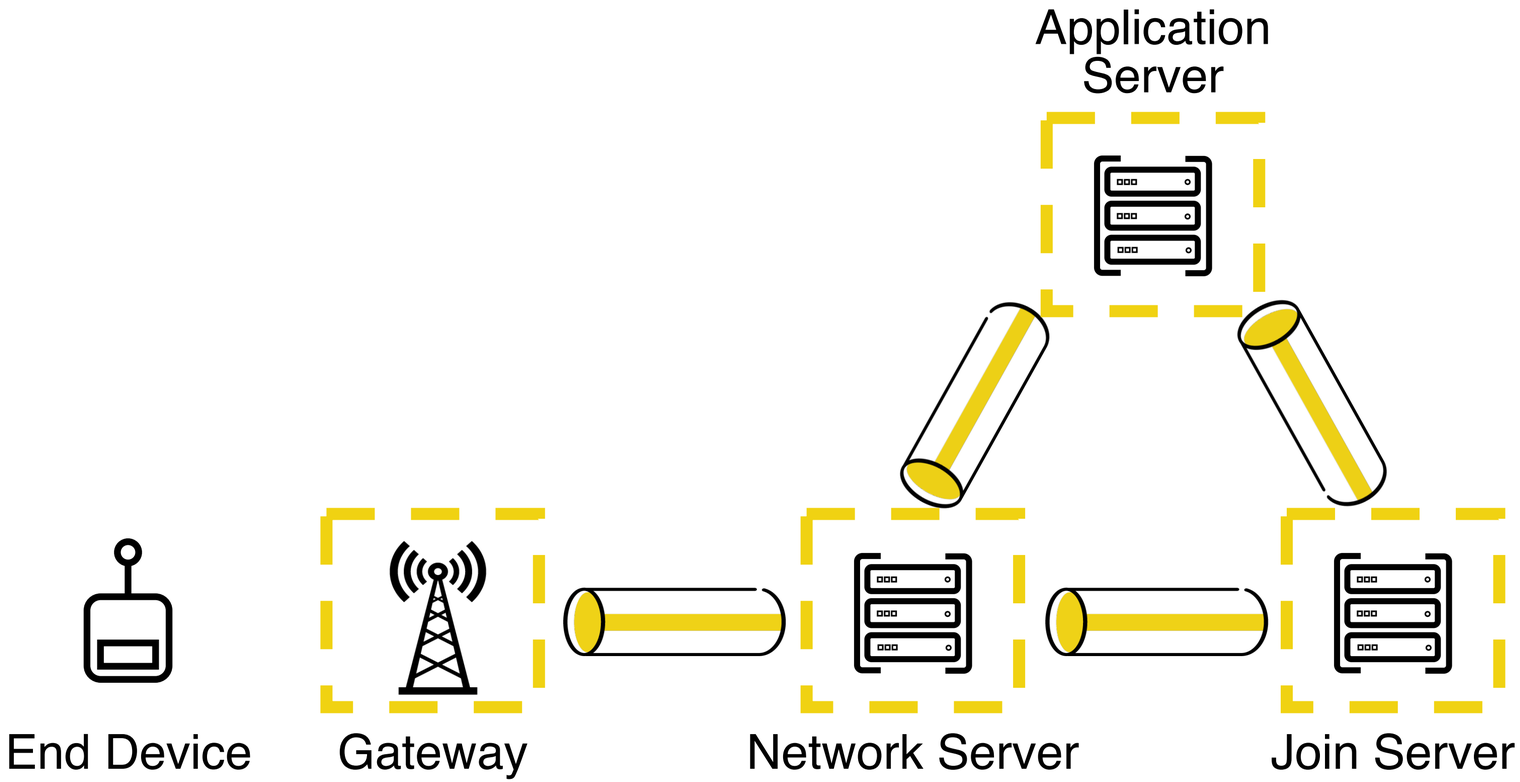
Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters



Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

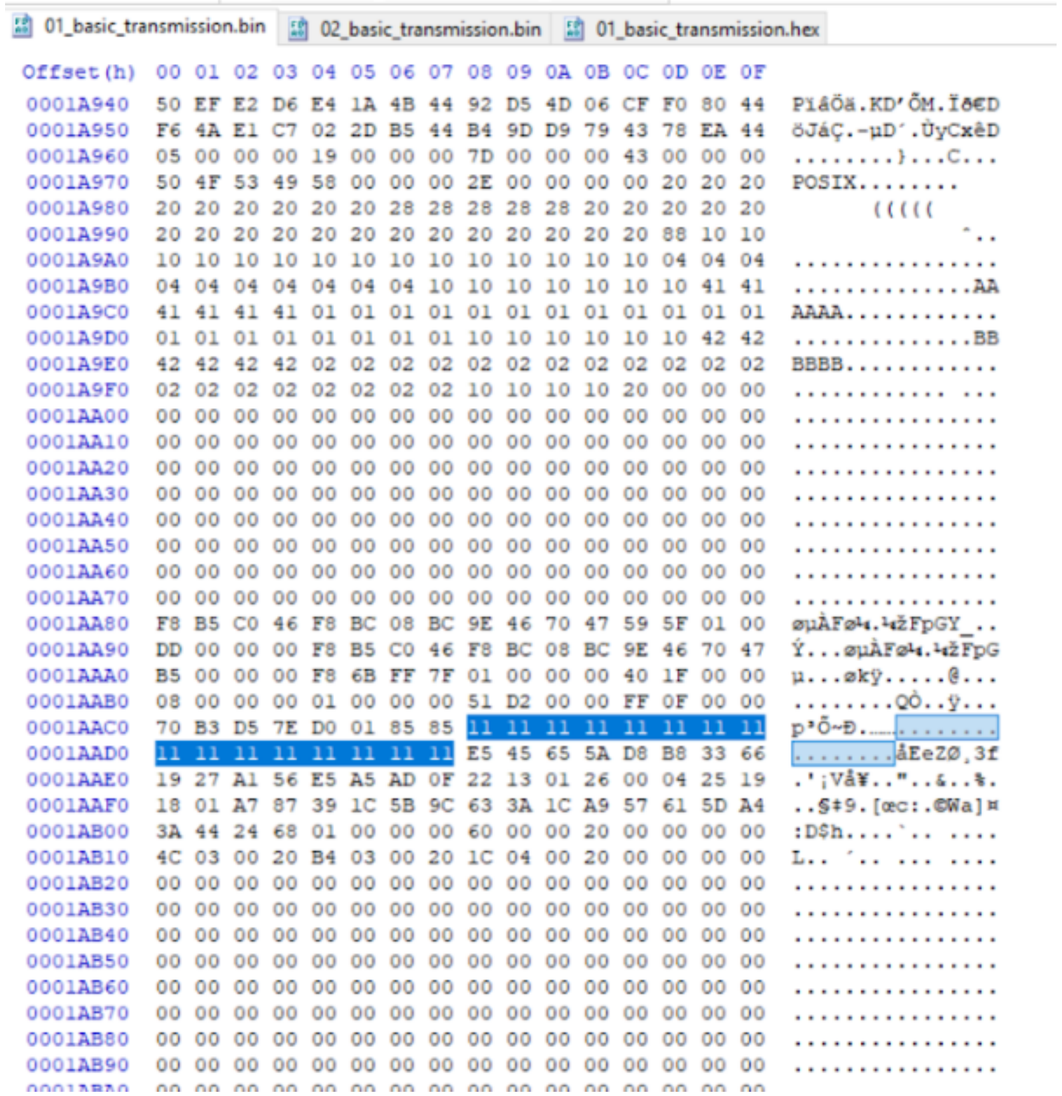
Implementation & Deployment Matters

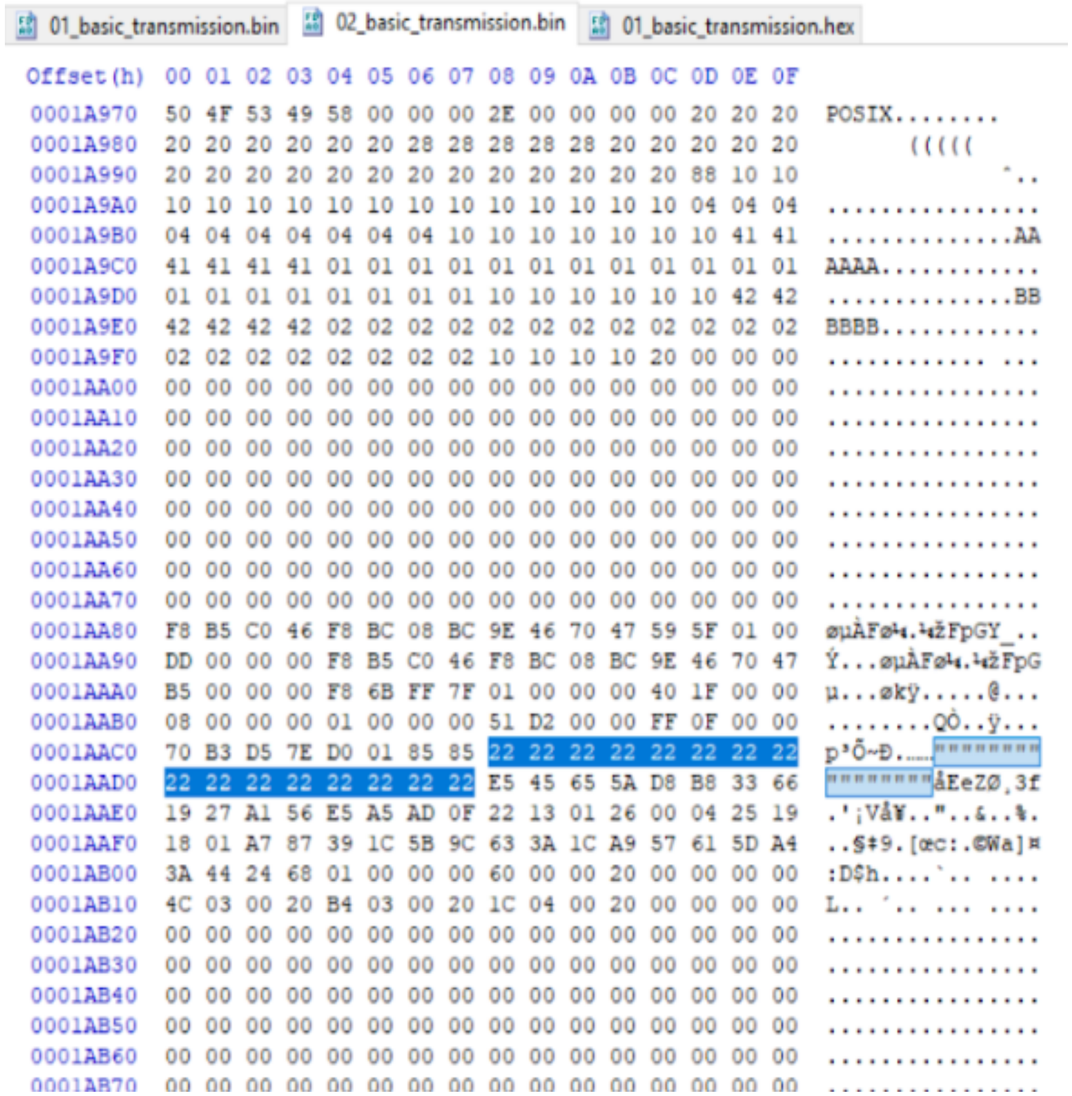


Backend infrastructure and communication security

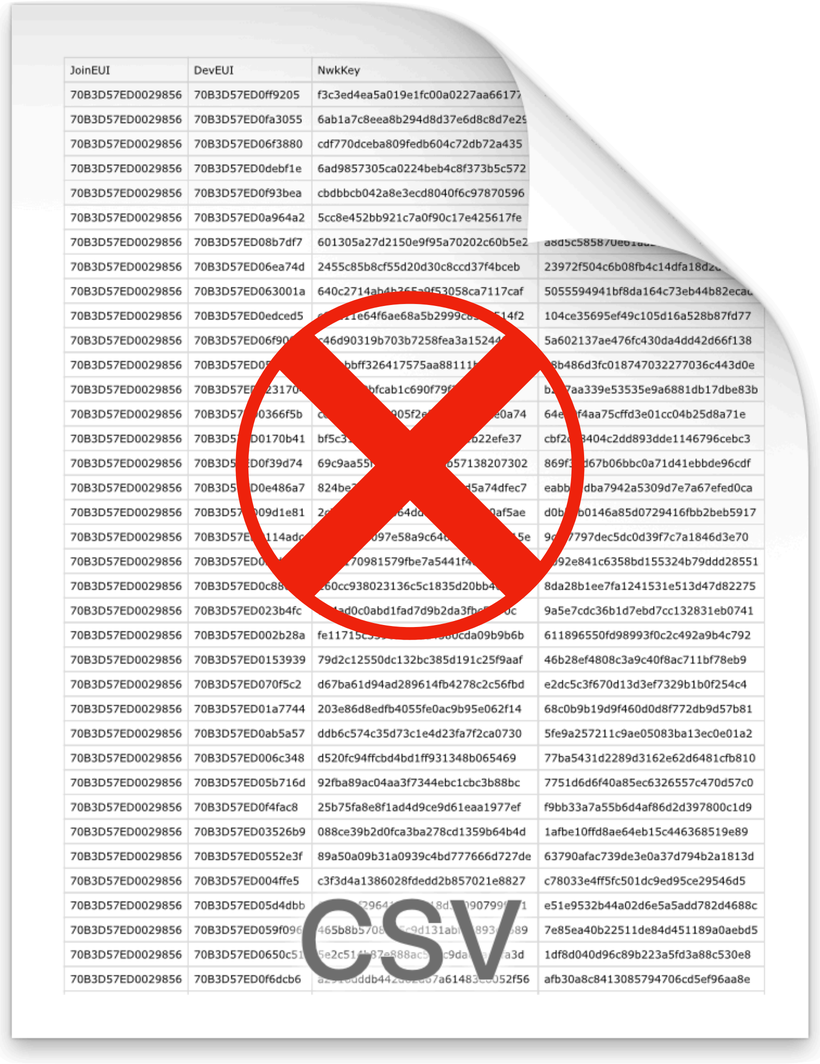
Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

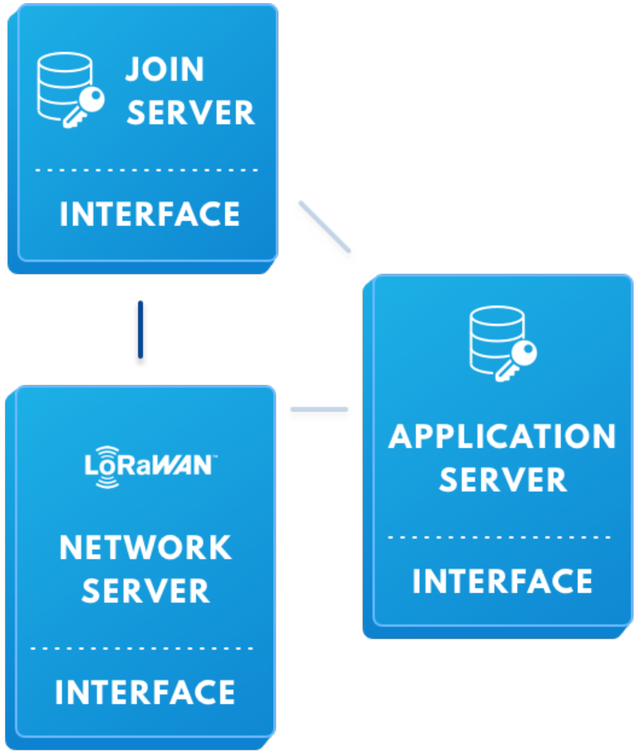
Implementation & Deployment Matters





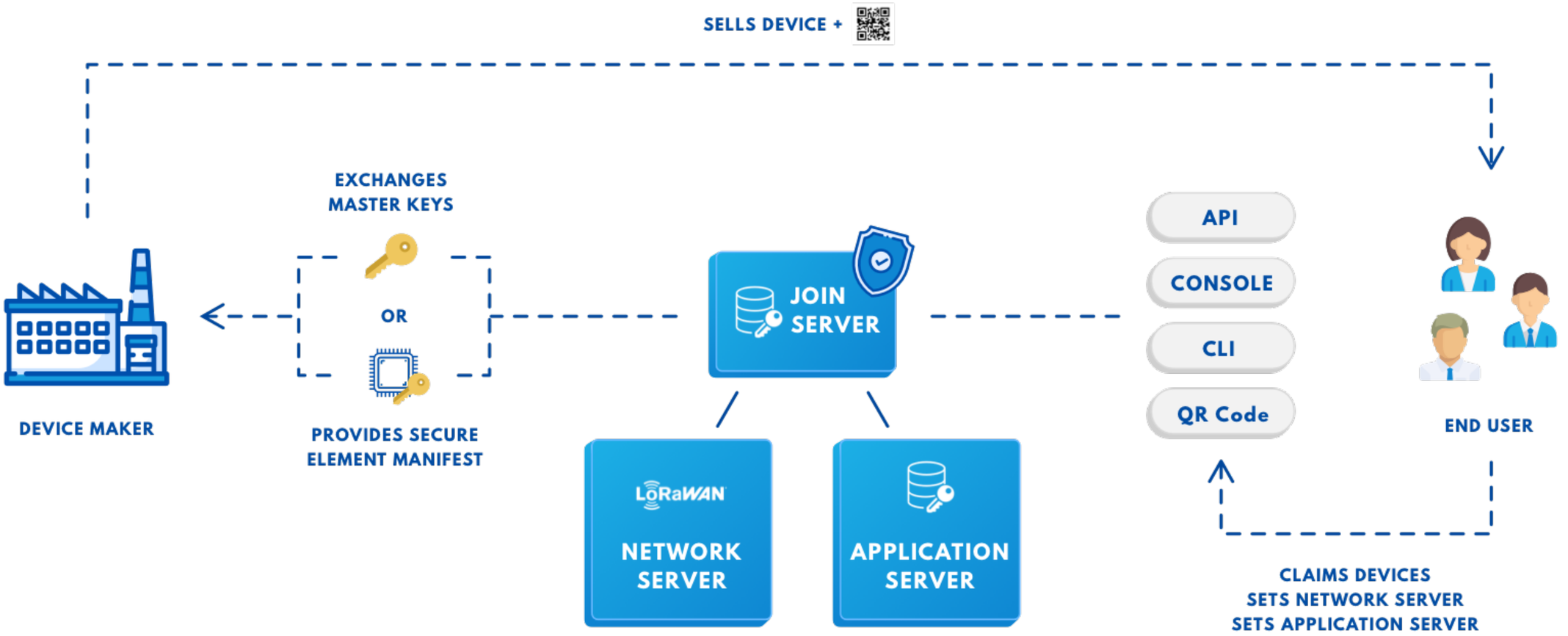
Implementation & Deployment Matters

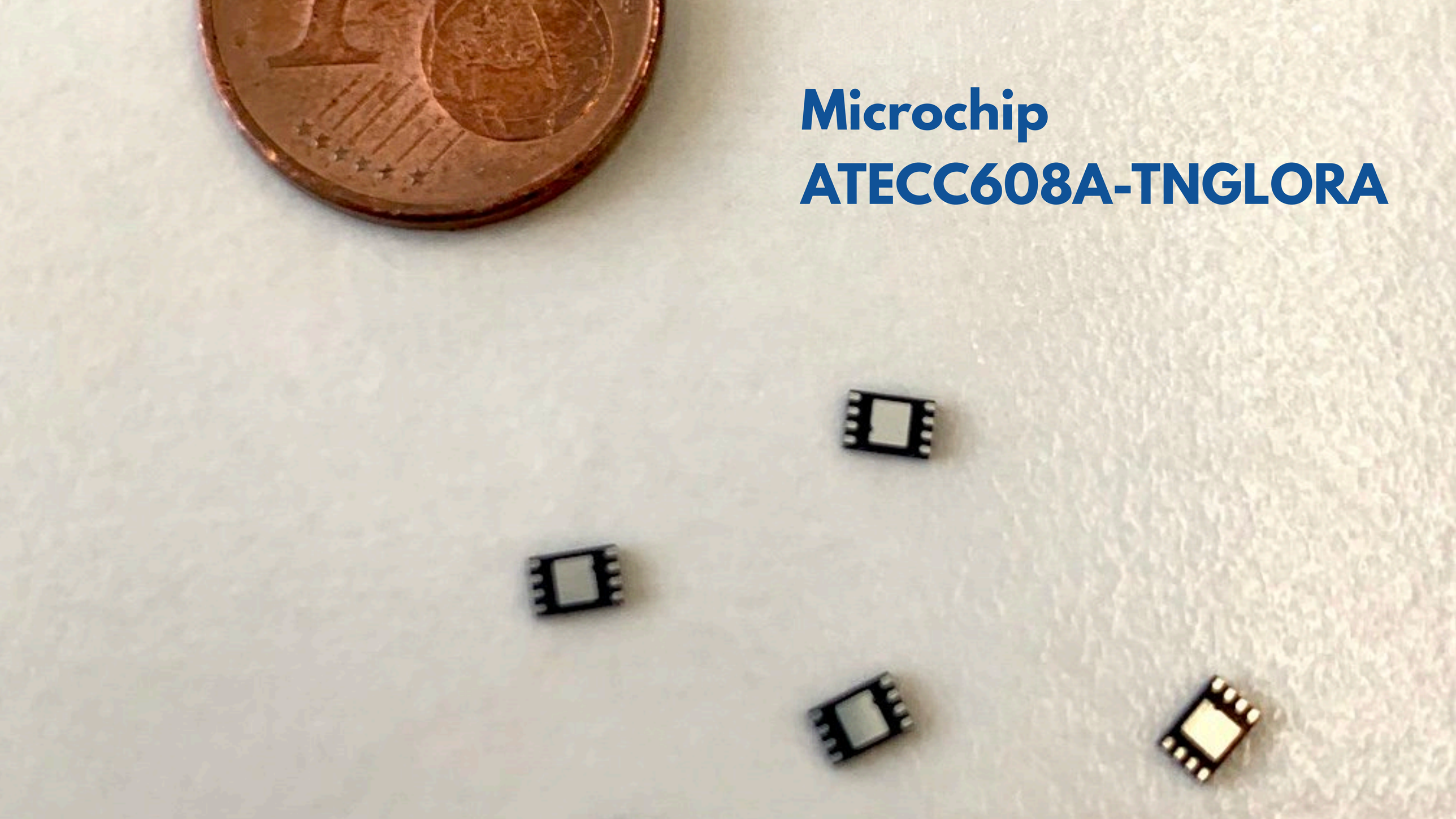




Implementation & Deployment Matters

The Things Industries developed the first LoRaWAN security solution using hardware secure elements. These secure elements are pre-provisioned by Microchip.




Microchip
ATECC608A-TNGLORA

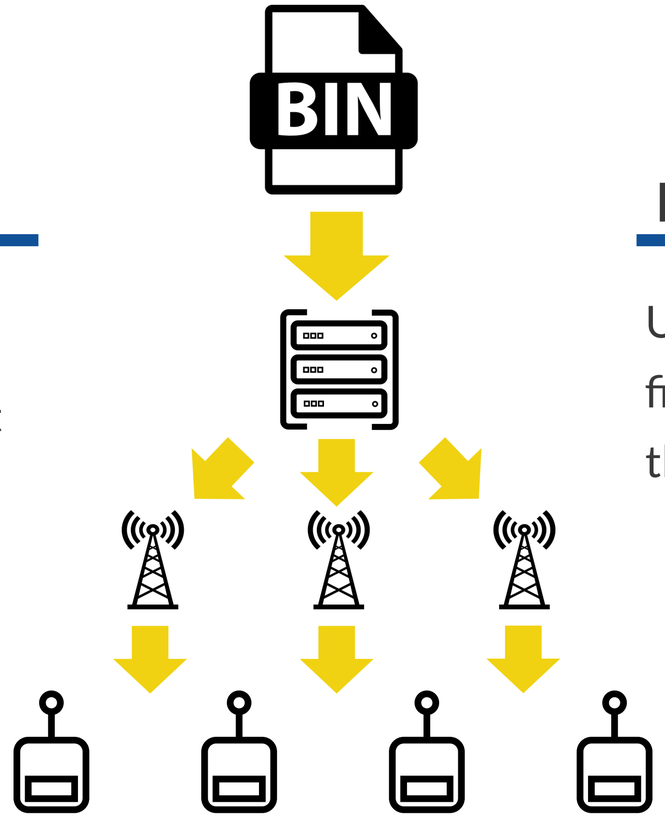
Firmware Updates over the Air (FUOTA)

Security for FUOTA

Signed firmware

Integrity-protected multicast delivery (using group key)

Integrity-protected unicast commands (using device key)

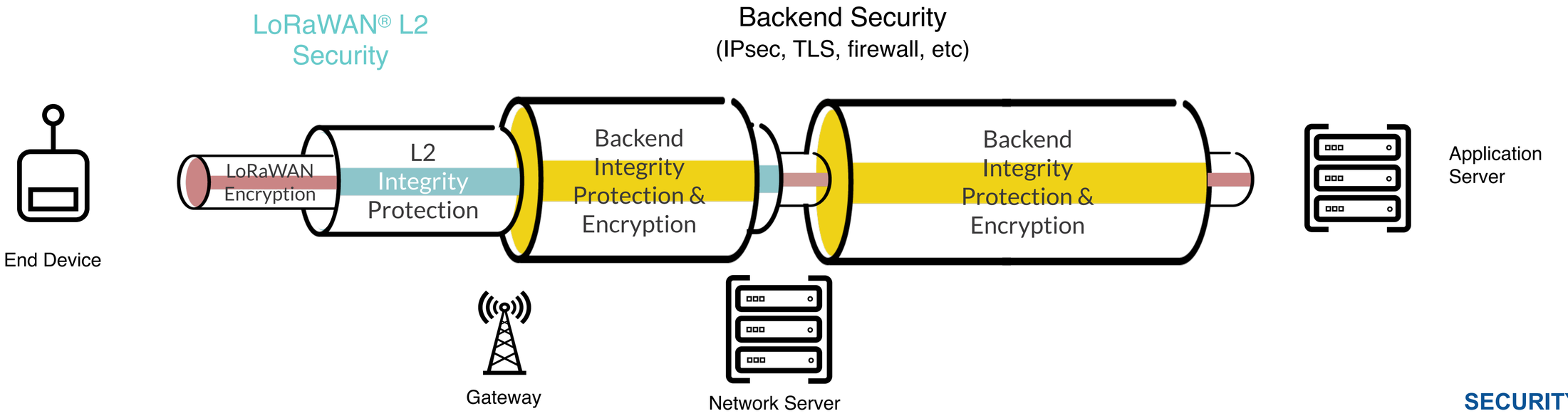


FUOTA for Security

Update device with software/ firmware (security) patches in the field

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Key Takeaways



Mutual end-point auth
Data origin auth
Integrity protection
Replay protection
Data encryption
…using AES-128

\+ FUOTA +

Hardware-level security (SE/HSMs)

SECURITY

Communication Technology	✓
Implementation	✓
Deployment	✓
OVERALL SOLUTION	✓

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

The Things Industries

Together with a team of professional developers we create the future of LoRaWAN. Pushing open standards and tools that help the LoRaWAN ecosystem build IoT applications.

https://join.thethingsindustries.com

Thank you