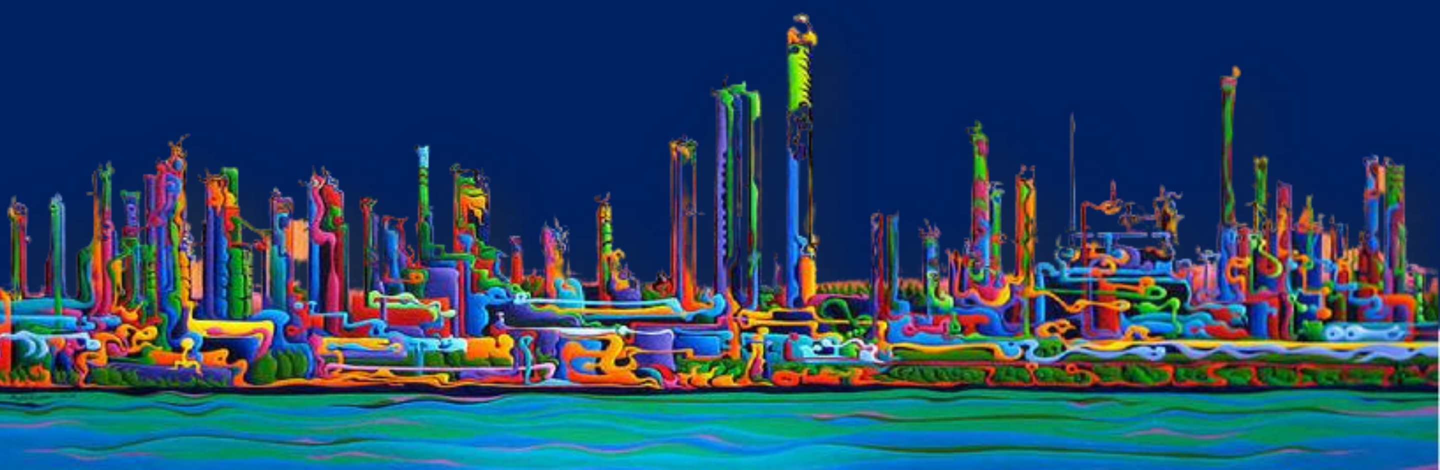
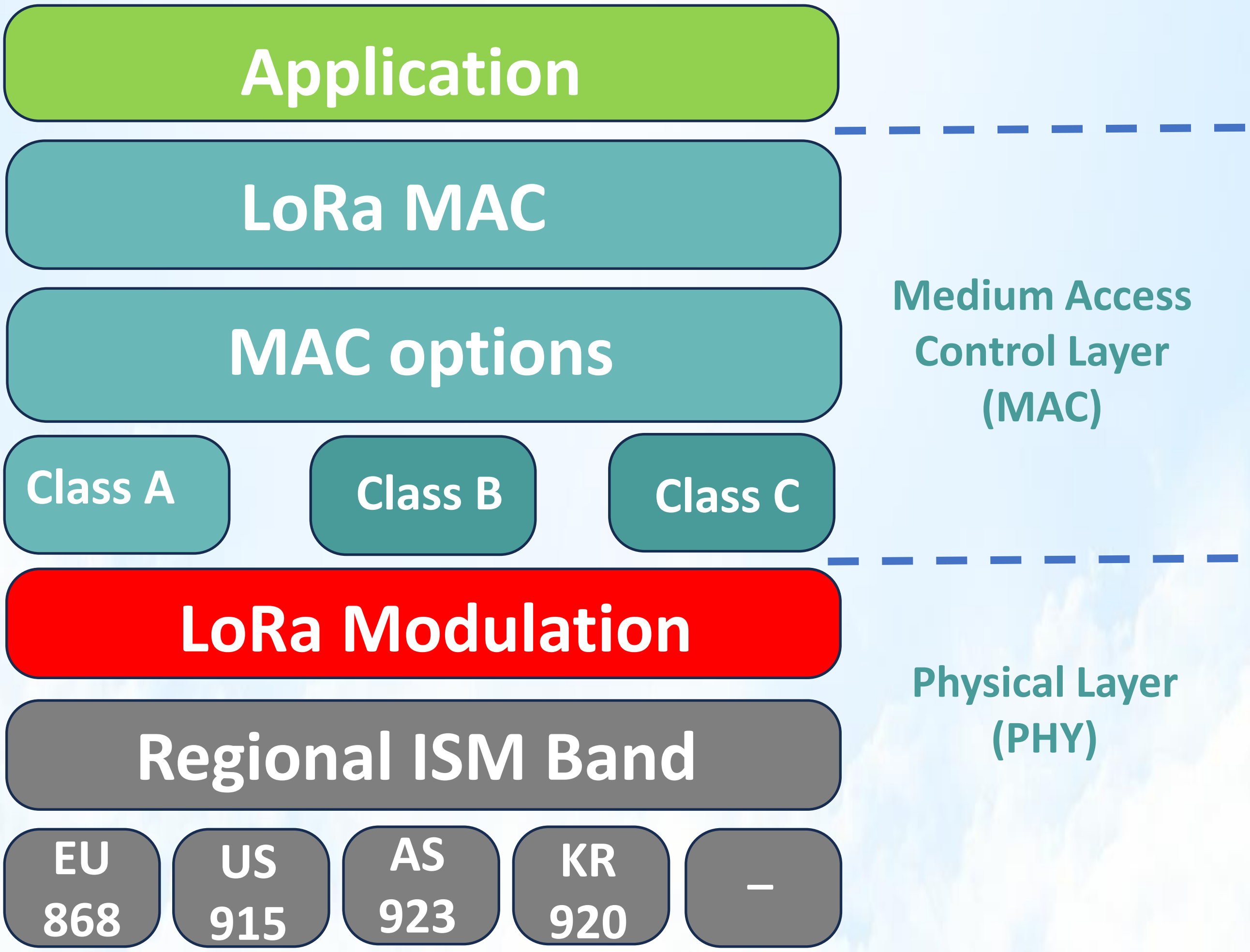
LoRa Alliance® Member

IS LORAWAN SECURE



OVERVIEW ON LORAWAN TECHNOLOGY

LoRa PHY is the physical layer commonly used by the LoRa Wide Area Network (**LoRaWAN**) Medium Access Control (MAC) stack, as shown in the OSI Network Model:



Application

LoRa MAC

MAC options

Class A

Class B

Class C

LoRa Modulation

Regional ISM Band

EU 868

US 915

AS 923

KR 920

–

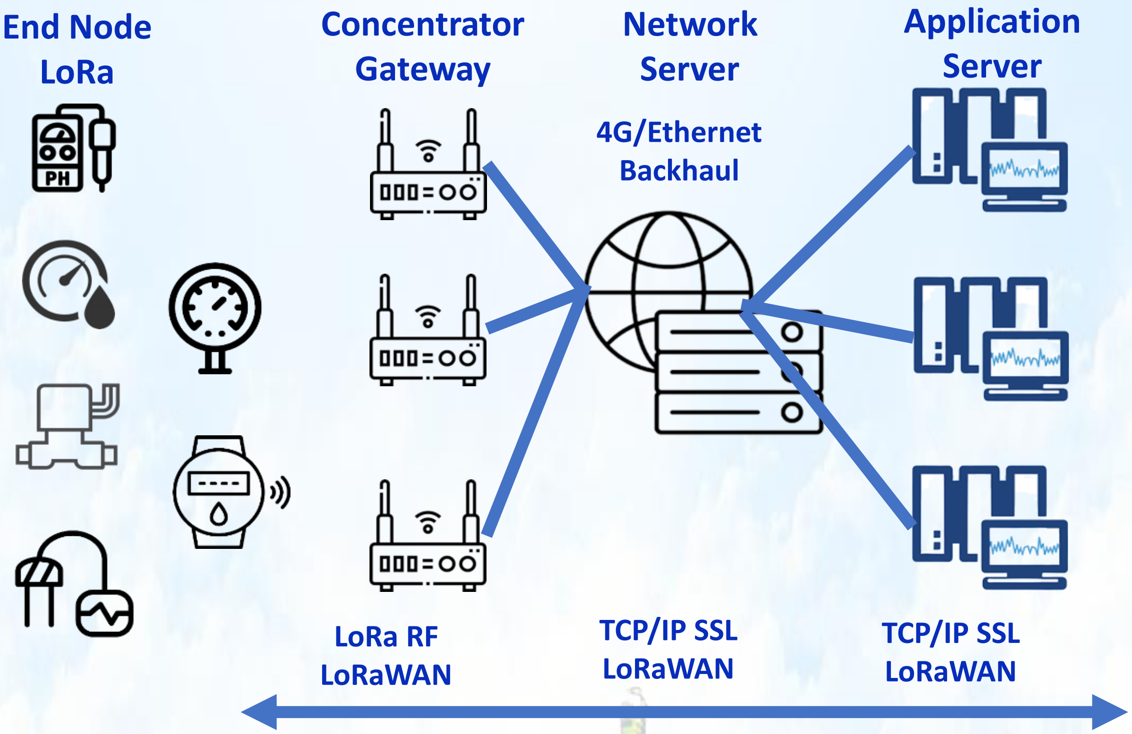
Medium Access Control Layer (MAC)

Physical Layer (PHY)

LoRa transmits signals using a proprietary CSS (CHIRP Spread Spectrum modulation technique to encode information. Invented initially for radar applications and then used by military and secure communications applications. CSS was adopted by IEEE for long-range and mobility for LR-WPAN standard, 802.15.4

OVERVIEW ON LORAWAN TECHNOLOGY

IOT devices can use LoRa PHY to transport messages, but since they do not provide native security mechanisms, developers need to implement their own security to protect messages from interception, injection, replay attacks, and other malicious activity. Another layer on top of LoRA PHY, called **LoRaWAN**, has been created to simplify communications and address these security problems



LORAWAN SECURITY

There are two different modes that define/compute keys for MAC frame payload encryption:

- OTAA (Over The Air Activation)
- ABP (Activation By Personalization)

regardless of the mode used with **LoRaWAN** communication, messages are protected by two session keys, **AppSKey** and **NwSKey**, which are used to encrypt messages

Indeed, the backend is exposed to the internet, which leaves it open to attacks (LFI, SQL injection, deserialization vulnerability, etc.). A malicious actor would be able to get the secret key, read the data, craft downlink packets, and more.

Hence Root Key Management is on top of all the security mechanisms.

SECURITY POINTS IN LORAWAN

Here are some security points to check in a **LoRaWAN** setup:

- Use randomly generated keys
- Avoid the exposition of key management servers and services (exposed key management service accessible on the internet)
- Preferably use HSM (Hardware Security Module) to keep the keys
- Preferably use OTAA mode and LoRa version 1.1.

FREQUENTLY ASKED QUESTIONS

- *Where are the LoRaWAN® security mechanisms specified?*

All security mechanisms are defined in the **LoRa Alliance®** specifications, which can be downloaded by the public from https://lora-alliance.org/resource-hub.

- *How do the LoRa Alliance specifications ensure secure operation of LoRaWAN networks?*

LoRaWAN supports mutual end-point authentication, data origin authentication, integrity and replay protection. It also enables end-to- end encryption of the application payload between the end-device and its counter-part on the network side, the Application Server.

LoRaWAN supports a mode of operation that allows encryption of the MAC commands.

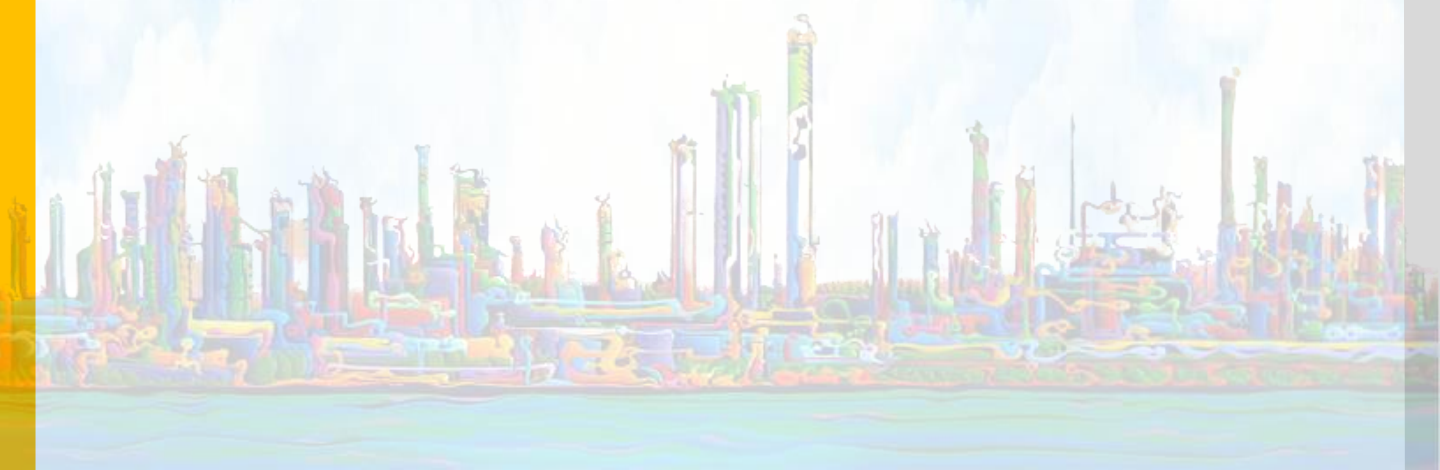
All of these procedures rely on the **Advanced Encryption Standard (AES) and use 128-bit** cryptographic keys and algorithms.

- *Are there any differences between the Activation by Personalization (ABP) and Over-the-Air-Activation (OTAA) methods in terms of security?*

LoRaWAN uses static root keys and dynamically-generated session keys. Root keys are only provisioned in OTAA end-devices. They are used to derive session keys when the OTAA end-device executes a Join Procedure with the network.

ABP end-devices are not provisioned with the root keys. Instead, they are provisioned with a set of session keys for a pre-selected network. The session keys remain the same throughout the lifetime of an ABP end-device.

OTAA should be preferred over ABP for end-devices in need of higher levels of security.



CONCLUSIONS

- LoRaWAN is by design very secure—authentication and encryption are, in fact, mandatory.

- LoRaWAN specification already offers dedicated end-to-end encryption to application providers.

- For more information about LoRaWAN security, please check out our updated Security FAQs, which address the common questions about how the specification has implemented security features.

SUSTECH
INTEGRATED TECHNOLOGIES

Office 1:
GF Office
Accelerator Building,
Masdar City

Office 2:
No. 101
Entrance No. 3
Rabdan Mall

T : +971 2 626 8774
info@sustechme.com
www.sustechme.com
P.O. Box 7123, Abu Dhabi, United Arab Emirates