WEBINAR SESSIONS

LORAWAN SECURITY

Johan Stokking

Tech Lead, The Things Network

JOHAN STOKKING

Tech Lead, The Things Network

johan@thethingsnetwork.org
@johanstokking

AGENDA

1. LoRa Security Fundamentals
2. Scope of Security in LoRaWAN
3. LoRaWAN Multicast
4. Join Server
5. Industrial LoRaWAN Deployments
6. Security in The Things Network Stack V3

THE THINGS NETWORK

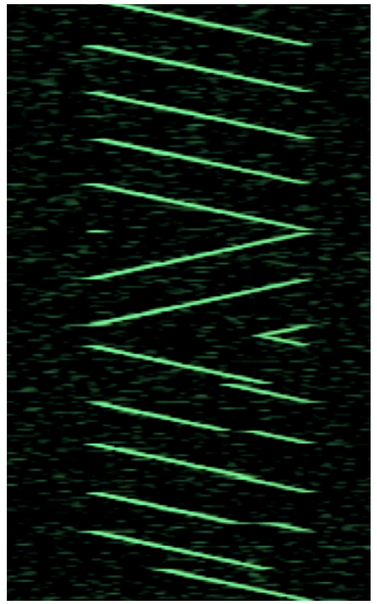
LORA PHY

It’s only physical and data link layer (only CRC)

LoRa PHY does not provide any security

Most reported breaches are LoRa PHY, not LoRaWAN

(Other reported breaches are bad use of LoRaWAN security)



THE THINGS NETWORK

LoRaWAN™ PROVIDES NETWORK, TRANSPORT, SESSION AND PRESENTATION LAYER MECHANISMS

THE THINGS NETWORK

SECURITY FOUNDATIONS

- Authenticity (network layer)
- Integrity (network layer)
- Confidentiality (network and application layer) through AES 128-bit ECB

THE THINGS NETWORK

ACTIVATING DEVICES

ABP vs OTAA

OTAA VS ABP

OTAA	ABP
New session on join	Fixed session
Supports rejoin, rekey	Requires persistent memory
Hand over roaming (in 1.1)	Keys cannot be changed

Use **OTAA**, unless there are very specific requirements, i.e. resource constraints

THE THINGS NETWORK

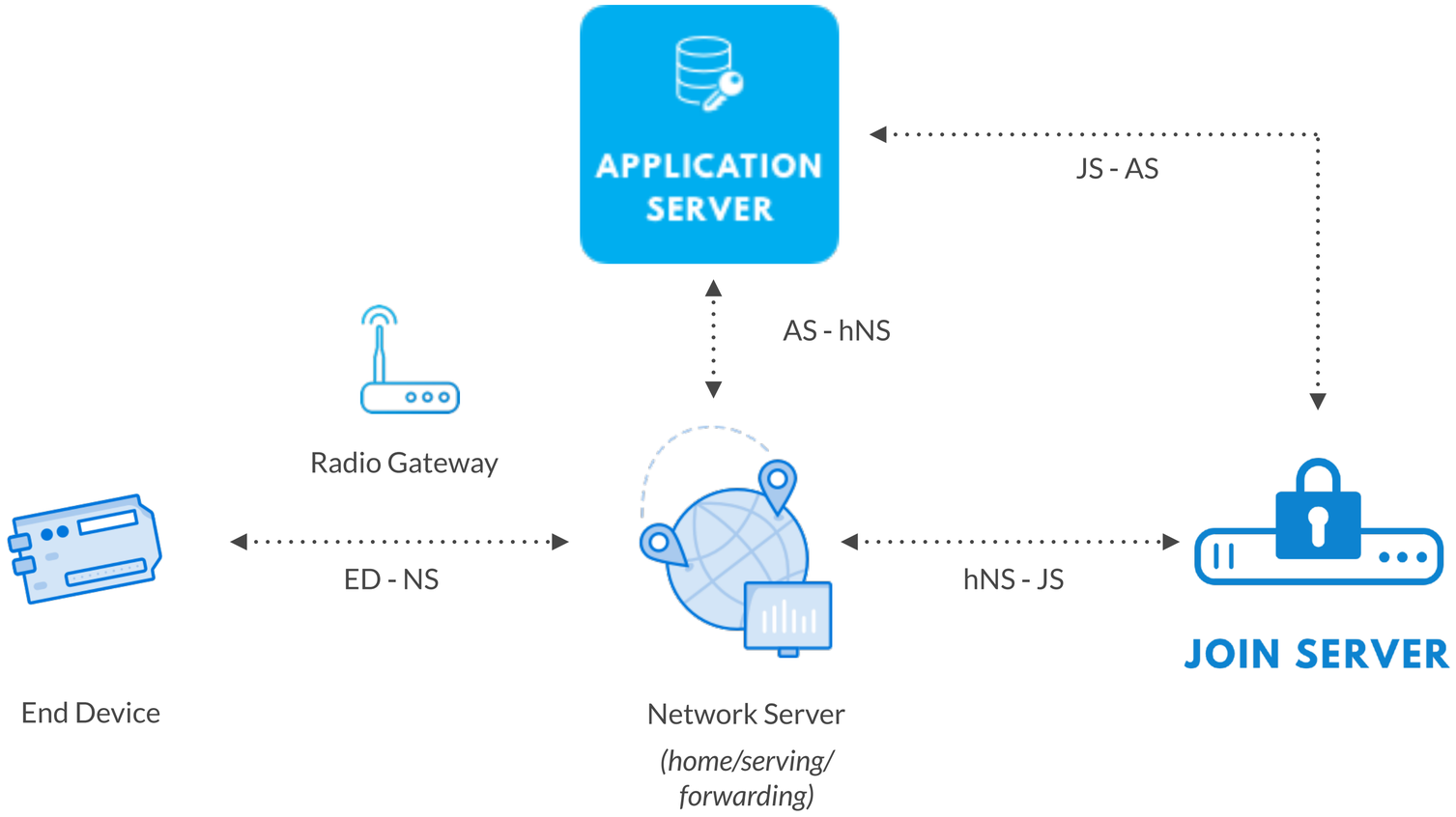
WEBINAR

See Webinar - What’s new in LoRaWAN 1.1

THE THINGS NETWORK

LORAWAN NETWORK REFERENCE MODEL

SIMPLIFIED VIEW



THE THINGS NETWORK

FUNCTIONAL SESSION KEYS

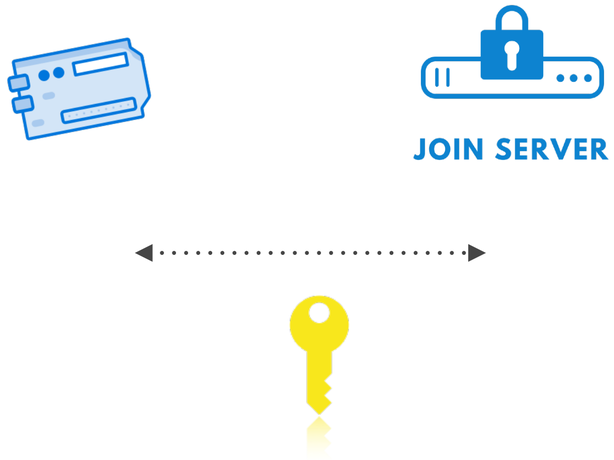
- LoRaWAN 1.1 introduces second root key (NwkKey, besides AppKey)
- Two new session keys
  - Integrity
    - `FNwkSIntKey` *(Forwarding Network Session Integrity Check)*
    - `SNwkSIntKey` *(Serving Network Session Integrity Check)*
  - Encryption
    - `NwkSEncKey` *(Network Session Encryption Key)*
    - `AppSKey` *(Application Session Key)*

THE THINGS NETWORK

SYMMETRIC KEYS - AES 128 BIT

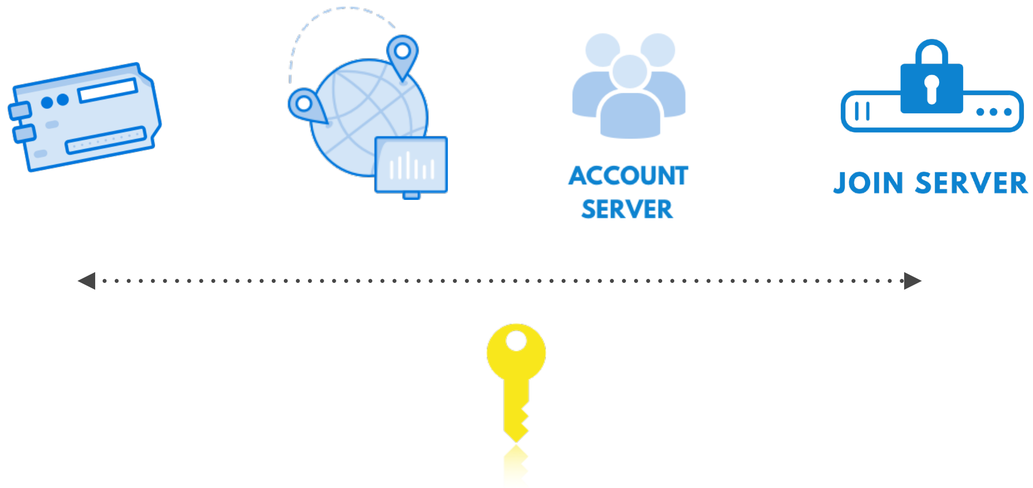
Secure solutions depend on compliance of all related components;

1



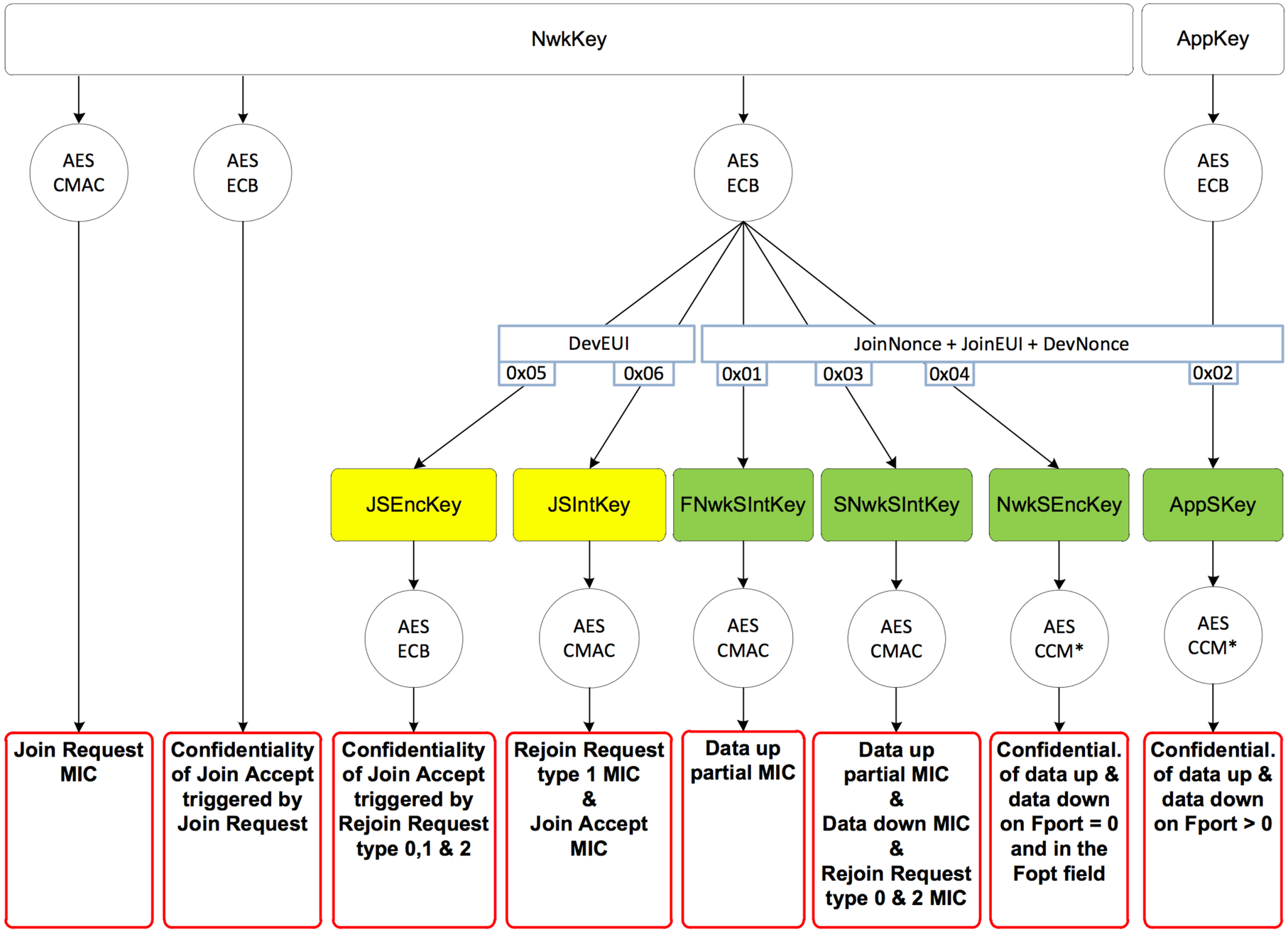
Root keys: AppKey and NwkKey

2



Session keys: FNwkSIntKey, SNwkSIntKey, NwkSEncKey, AppSKey

THE THINGS NETWORK



THE THINGS NETWORK

OTHER SECURITY FEATURES

- **Link check** allows end device to determine link availability and quality parameters
- **Confirmation of data messages** allows end devices to ensure that packets have been received by the network server, supporting at-least-once delivery (LoRaWAN 1.1)
- **Channel utilization optimization** through adaptive data rate (ADR) reduces packet loss
- **Join and data message replay detection** avoids triggering duplicate events upstream and bringing end devices in invalid states (LoRaWAN 1.1)

THE THINGS NETWORK

WEBINAR

See Webinar - What’s new in LoRaWAN 1.1

THE THINGS NETWORK

PUBLIC INFORMATION IN LORAWAN

- **JoinEUI/DevEUI** in join request
  - **JoinEUI** refers to Join Server, i.e. tells attacker where the root keys are
  - **DevEUI** may indicate the LoRaWAN module and version or end device module and version
- Device address (4-bytes, reusable), indicates LoRaWAN network
- Frame counter
- Length of application payload and port
- Sometimes: MAC commands

THE THINGS NETWORK

MONITORING A PARKING LOT

- Join requests from parking sensors may indicate the brand, model and version of the parking sensors (DevEUI)
- The device addresses and frame counters may indicate
  - The network operator
  - An estimation of the number of parking sensors (unique DevAddr + FCnt behavior)
- Parking activity if it can be derived from message timing, payload length and/or port

THE THINGS NETWORK

TIPS TO MASK ACTIVITY

- Use a DevEUI that doesn’t relate to the end device brand, model and version
- Use a fixed payload length and do not use FPort as sensitive data field
- Consider decoupling physical events (i.e. car drives away) from sending a message, i.e. jitter or periodic status messages

THE THINGS NETWORK

MULTICAST SECURITY

- Multicast: send downlink messages to multiple devices (class B or C)
- One or more (temporary) multicast security contexts, next to the unicast security context
- All devices in the multicast group use the same security context, i.e. same device address and session keys
- If one end device gets compromised, an attacker can send downlink too as security is symmetric
- Application layer mechanism
- Specified in Remote Multicast Setup over LoRaWAN v1.0.0 RPD

THE THINGS NETWORK

SECURITY MEASURES FOR MULTICAST

- Limited number of messages per multicast session
- Limited time when a class B or C session stays active
- Enforce that all end devices in the multicast group use a hardware secure module (HSM)
  - The multicast key **McKey** to derive session keys from is sent encrypted with a per-device lifetime key encryption key **McKEKey**
  - The McKEKey is shared out-of-band with the application
  - The application may group devices for multicast if the McKEKey is stored in a HSM
  - Note: end devices are still required to store the decrypted McKey in the HSM too

THE THINGS NETWORK

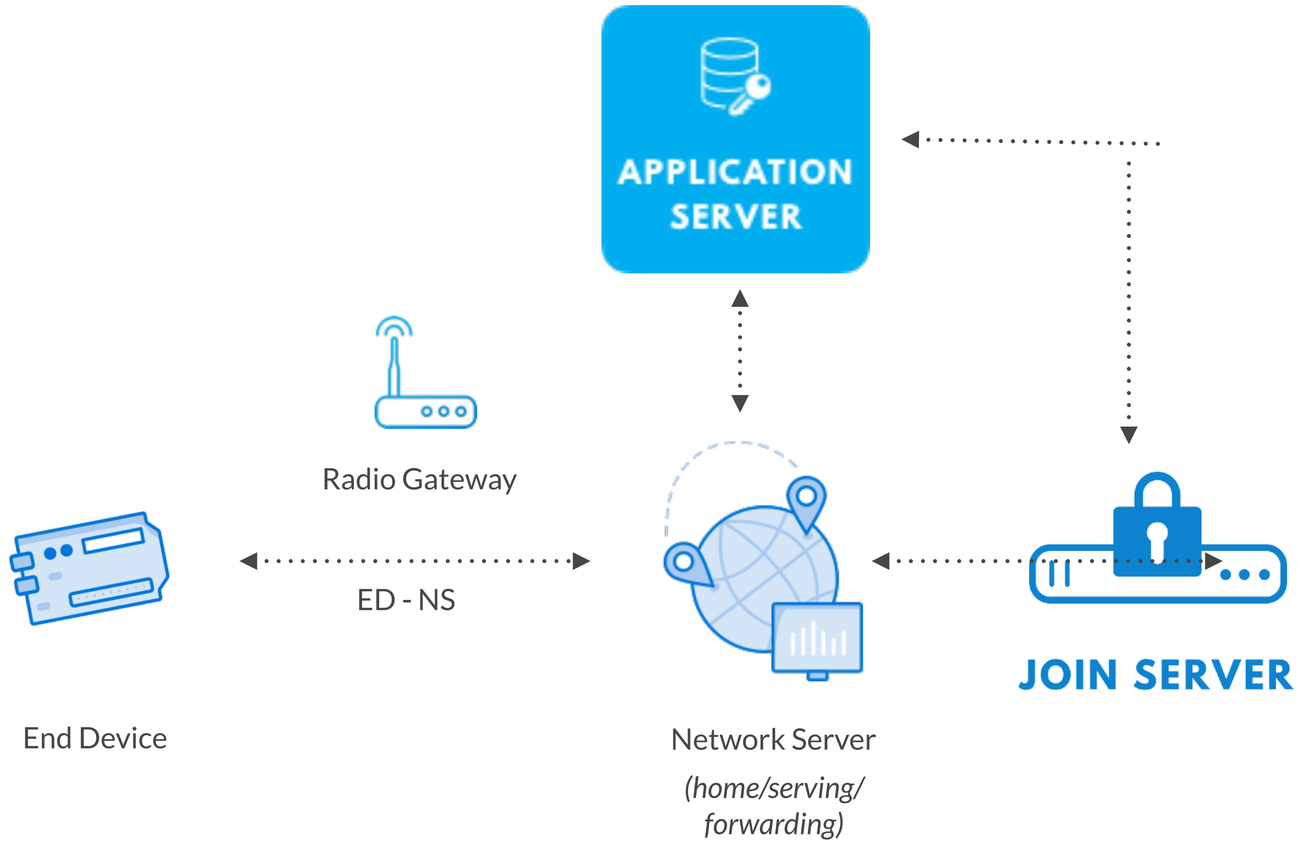
SECURING LORAWAN DEPLOYMENTS

RED FLAGS 🚩 🚩

- Use of ABP: not secure; keys cannot be changed, must be shared with network operator
- Keys printed on paper or sent by email; keys should not be visible (use HSM), paper trail is impossible to clear
- Unable to choose a Join Server or operate your own: platform lock-in, potentially unsafe storage of end device root keys
- Unable to choose an Application Server or operate your own: application data may get compromised
- Same keys for multiple end devices: end devices need unique keys
- Hardcoded keys in end device: end devices should use a HSM

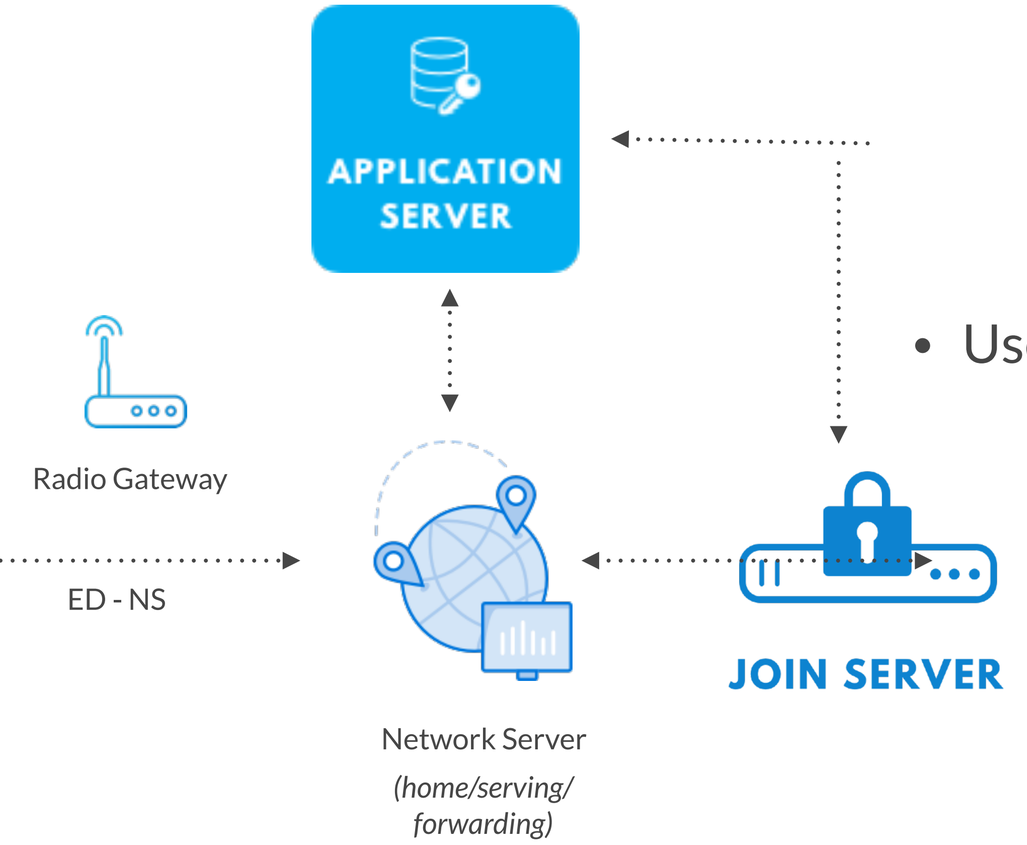
THE THINGS NETWORK

SECURING LORAWAN DEPLOYMENTS



THE THINGS NETWORK

SECURING LORAWAN DEPLOYMENTS



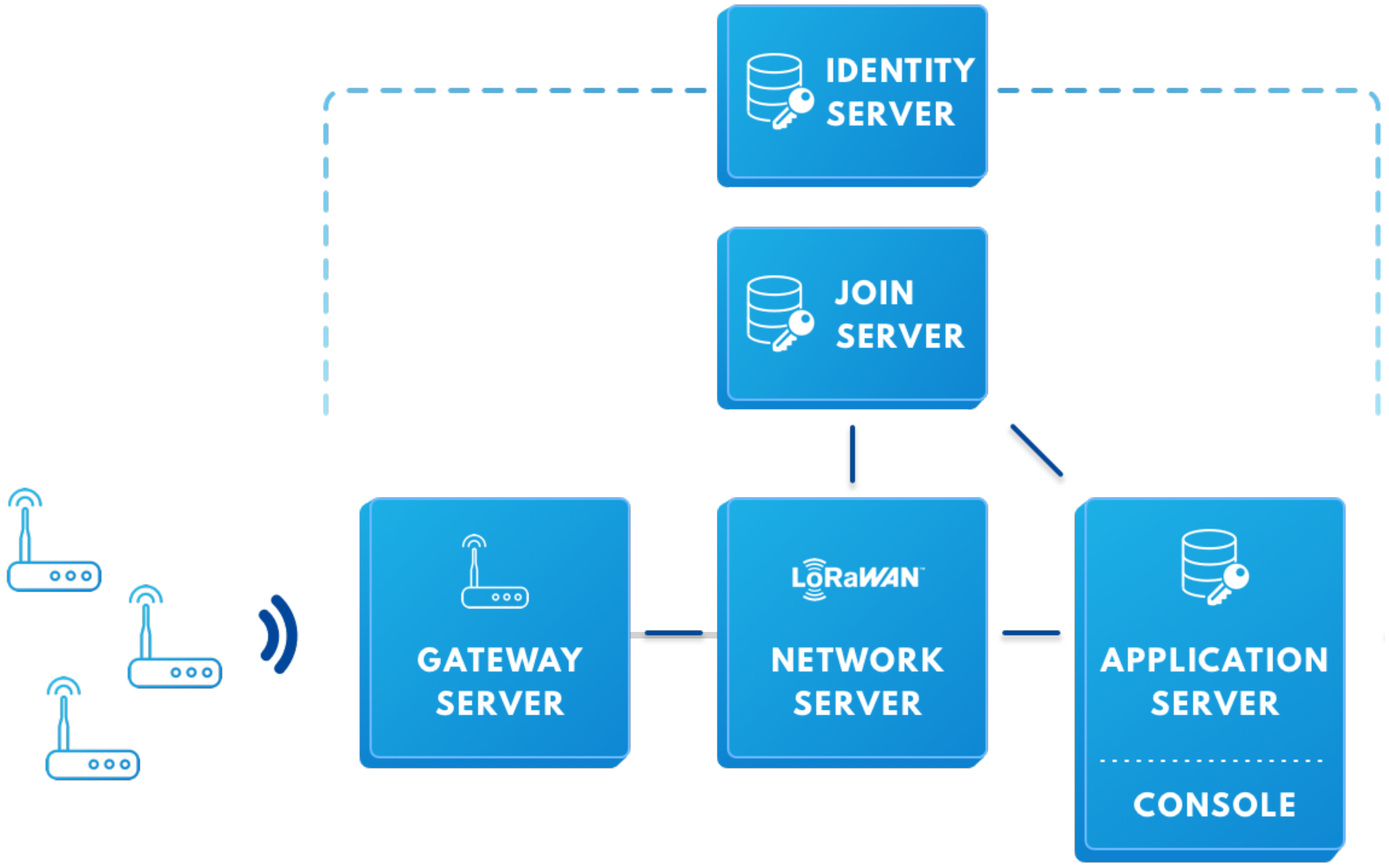
- Use a network solutions provider that follows the LoRaWAN NRM and implement the LoRaWAN Backend Interfaces 1.0
  - Join Server generates session keys from root keys, and sends them encrypted to the NS and AS
  - Network Server handles MAC layer and has only access to network session keys
  - Application Server has only access to application session key
- Use an end device with hardware secure module (HSM)
  - Performs LoRaWAN operations; i.e. neither the root keys nor the session keys are readable
  - Keys are provisioned by the manufacturer or distributor on a Join Server

THE THINGS NETWORK

HOW ARE ROOT KEYS PROVISONED?

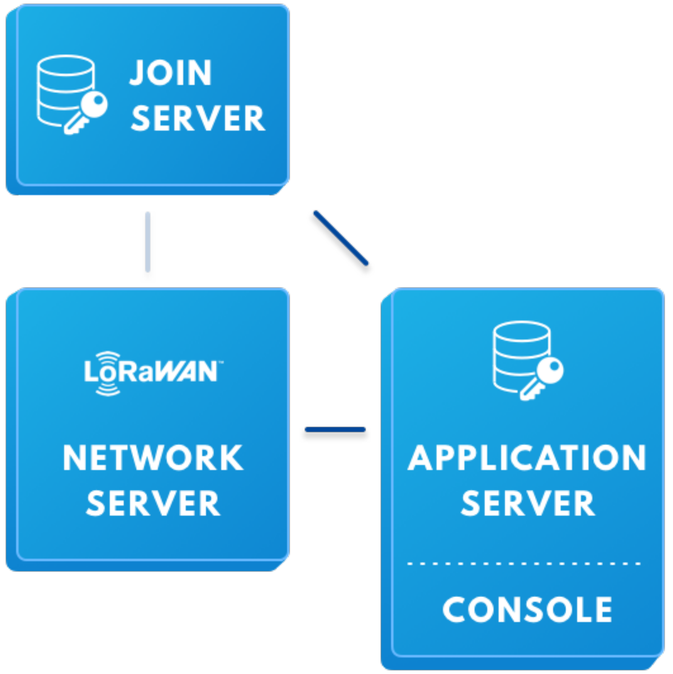
- LoRaWAN root keys and session keys are symmetric
- LoRaWAN root keys should not be exchanged
- Instead, the end device key provisioner and Join Server provider should share a master key
  - End device key provisioner may be the end device's HSM manufacturer, the end device manufacturer or the distributor
  - The master key should not be readable to anyone
  - Join Server provider generates key in HSM, encrypts it with end device key provisioner's HSM's public key and sends the key envelope to the manufacturer
  - Manufacturer decrypts the key envelope in its HSM with its private key
  - From the master key, the JoinEUI, the DevEUI and other out-of-band information, the manufacturer's and Join Server's HSM generate the same (i.e. symmetric) per-device LoRaWAN root keys
- Alternatively, the end device may be provisioned with the manufacturer's Join Server for "first join", which reprovisions the end device out-of-band to another Join Server for "second join"

THE THINGS NETWORK


IDENTITY SERVER
JOIN SERVER
GATEWAY SERVER
LoRaWAN
NETWORK SERVER
APPLICATION SERVER
CONSOLE

V3 JOIN SERVER AND SECURITY

- Stores the LoRaWAN root keys and derives session keys
- You can deploy the Join Server inside or outside a V3 cluster, i.e. a private cloud or on-premises in a trusted domain
- Control your security keys in your Join Server while using any V3 deployment scenario
- Gives you the power to switch V3 clusters: public to private, private to public and private to private



THE THINGS NETWORK

QUESTIONS?

johan@thethingsnetwork.org
@johanstokking