Actility
Connecting with intelligence

LoRaWAN Security

Alper Yegin

Director of Standards and Advanced Technology Development, Actility

Technical Committee Co-chair and Vice-Chair, LoRa Alliance

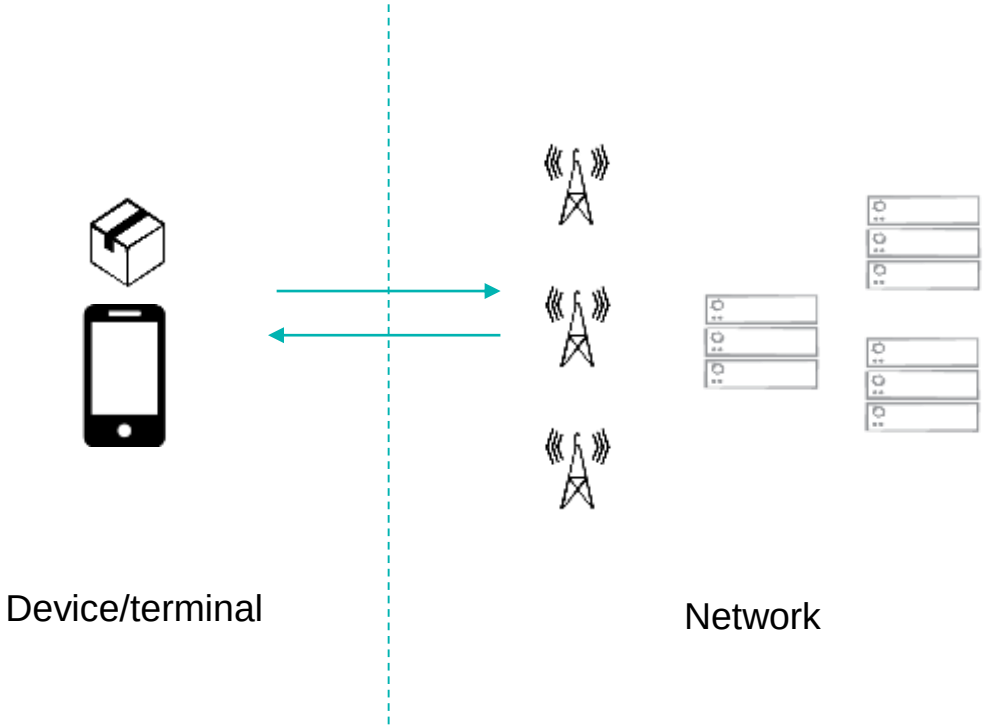
Is LoRaWAN secure?

Actility

How are the LoRaWAN protocol/networks secured?

Actility

General Wireless Security

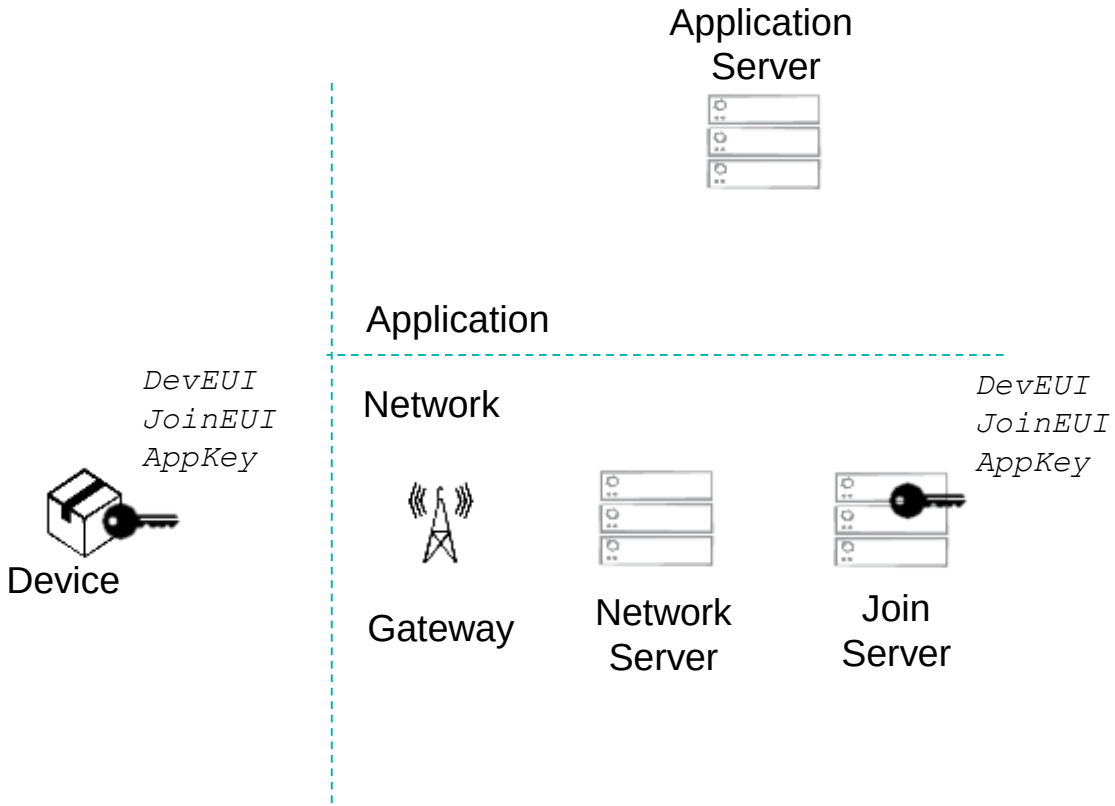


Threats	Remedies (tools)
Unauthorized access	Mutual end-point authentication
Spoofing	Data origin authentication
	Replay protection
Modification	Integrity protection
Eavesdropping	Encryption

… using cryptographic algorithms with strong keys

Actility

Mutual End-point Authentication



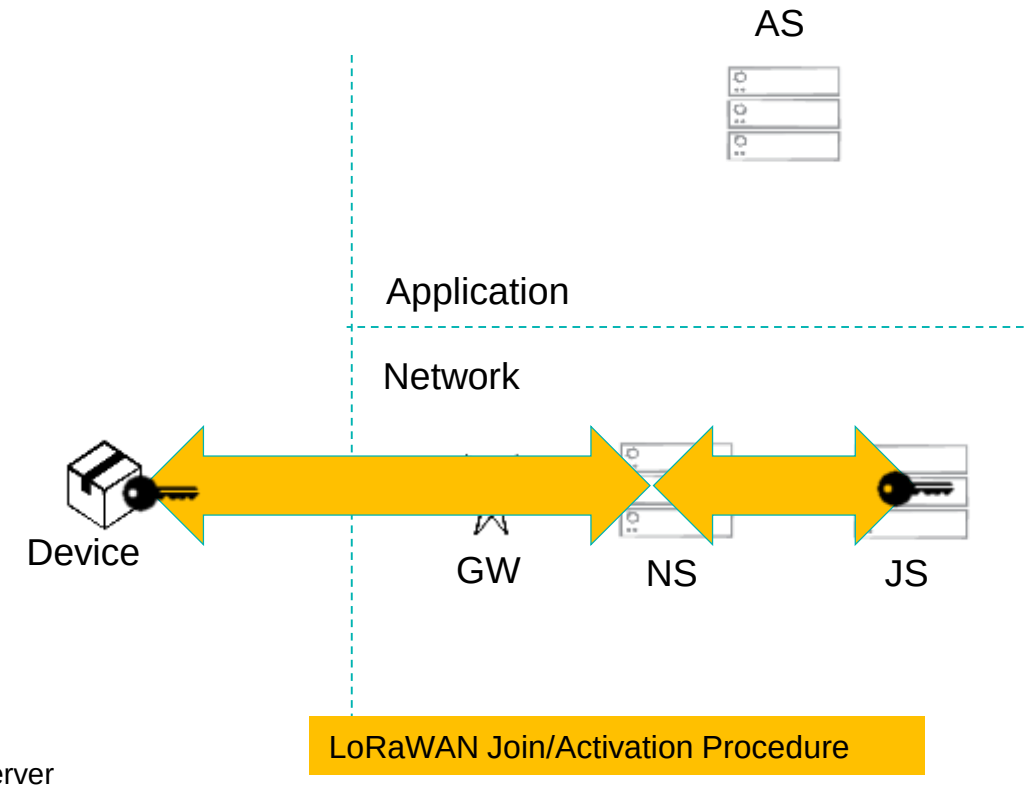
Using Advanced Encryption Standard (AES) with 128-bit symmetric keys and algorithms

AppKey is random and per-device root key (cryptographic isolation)

DevEUI: Device Extended Unique Identifier
JoinEUI: Join server Extended Unique identifier (replaces AppEUI in earlier specs)
Note -- Depicting LoRaWAN 1.0.x for brevity

Actility

Mutual End-point Authentication



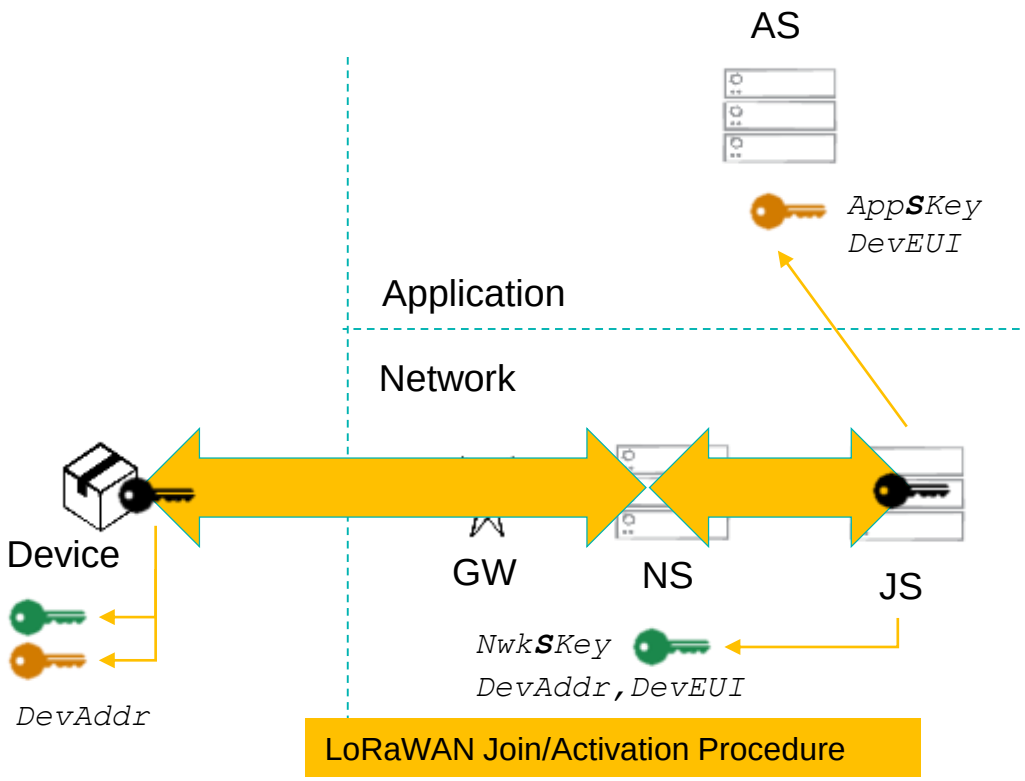
Using Advanced Encryption Standard (AES) with 128-bit symmetric keys and algorithms

AppKey is random and per-device root key (cryptographic isolation)

AS: Application Server
JS: Join Server
NS: Network Server
GW: Gateway

Actility

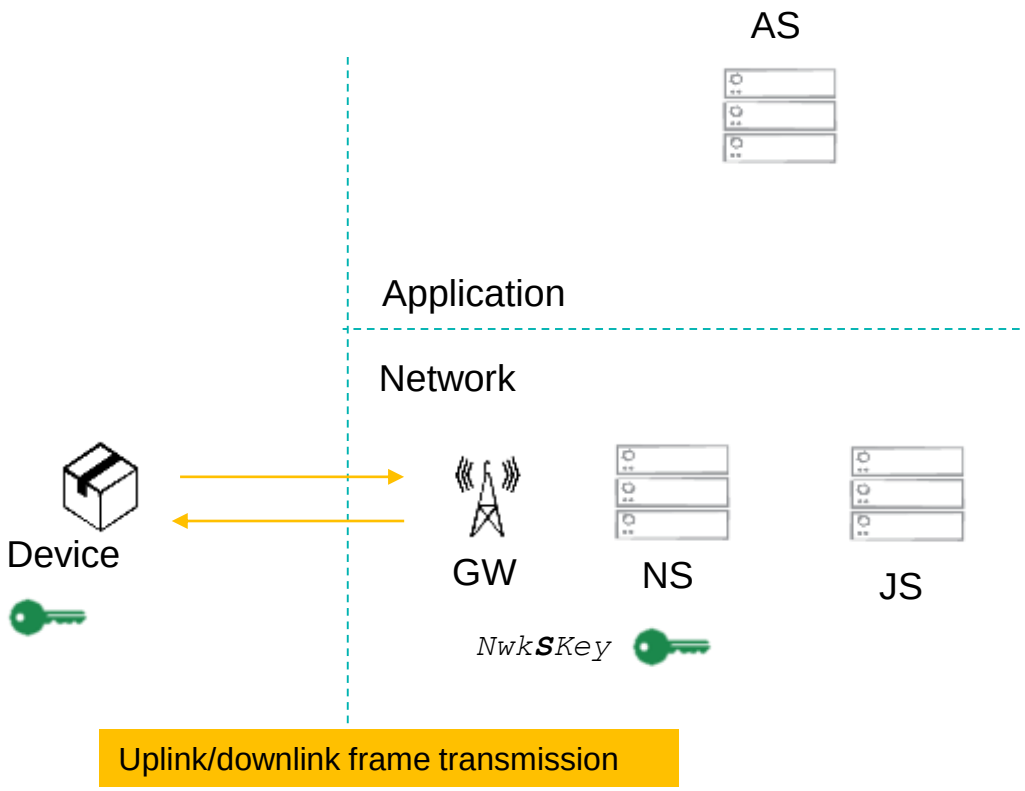
Session Key Generation and Delivery

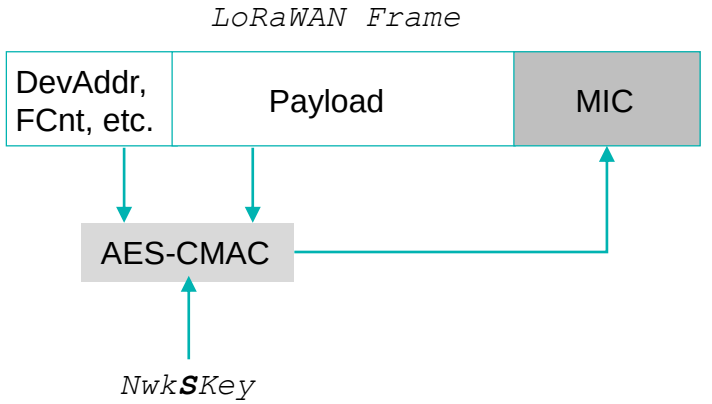


AES-128 symmetric session keys

Actility

Data Origin Authentication, Integrity and Replay Protection

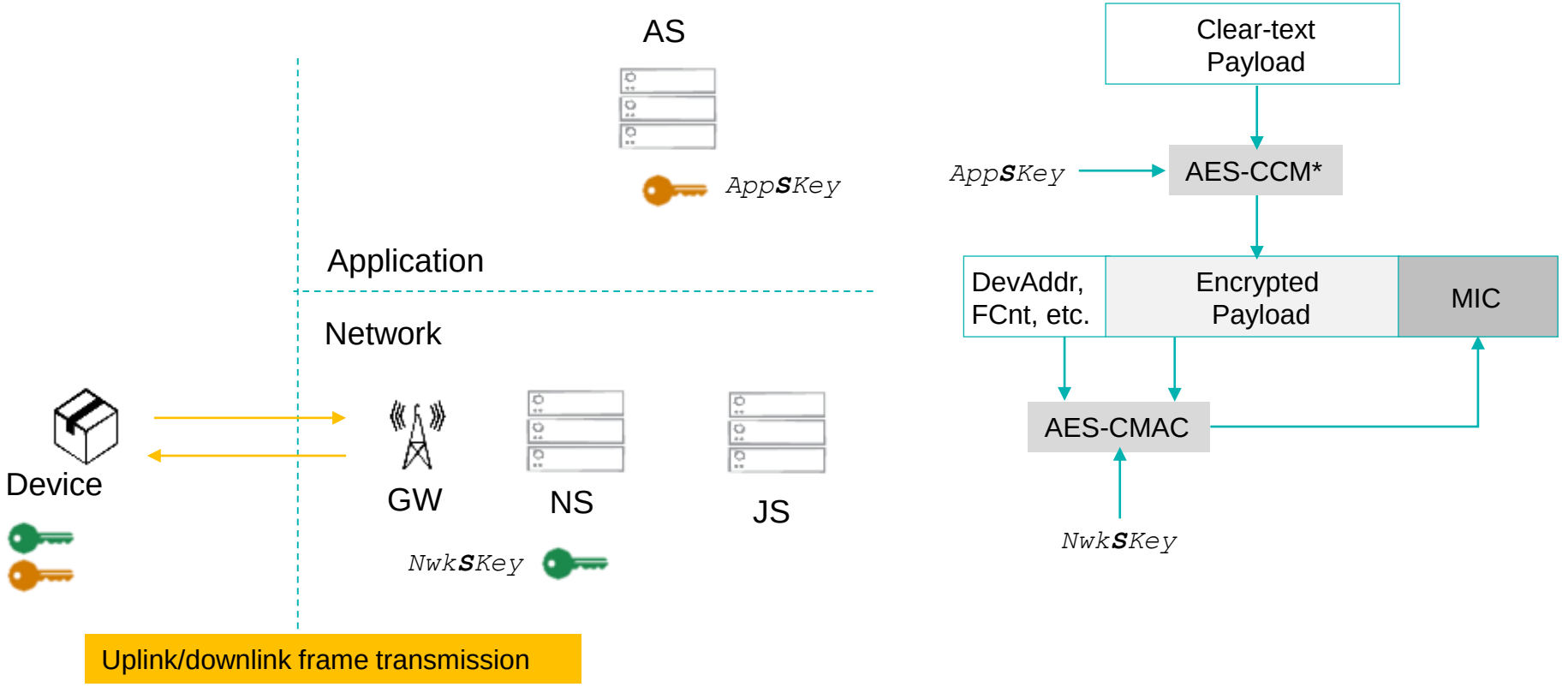




MIC: Message Integrity Code
AES-CMAC: AES Cipher-based Message Authentication Code (tools.ietf.org/html/rfc4493)

Actility

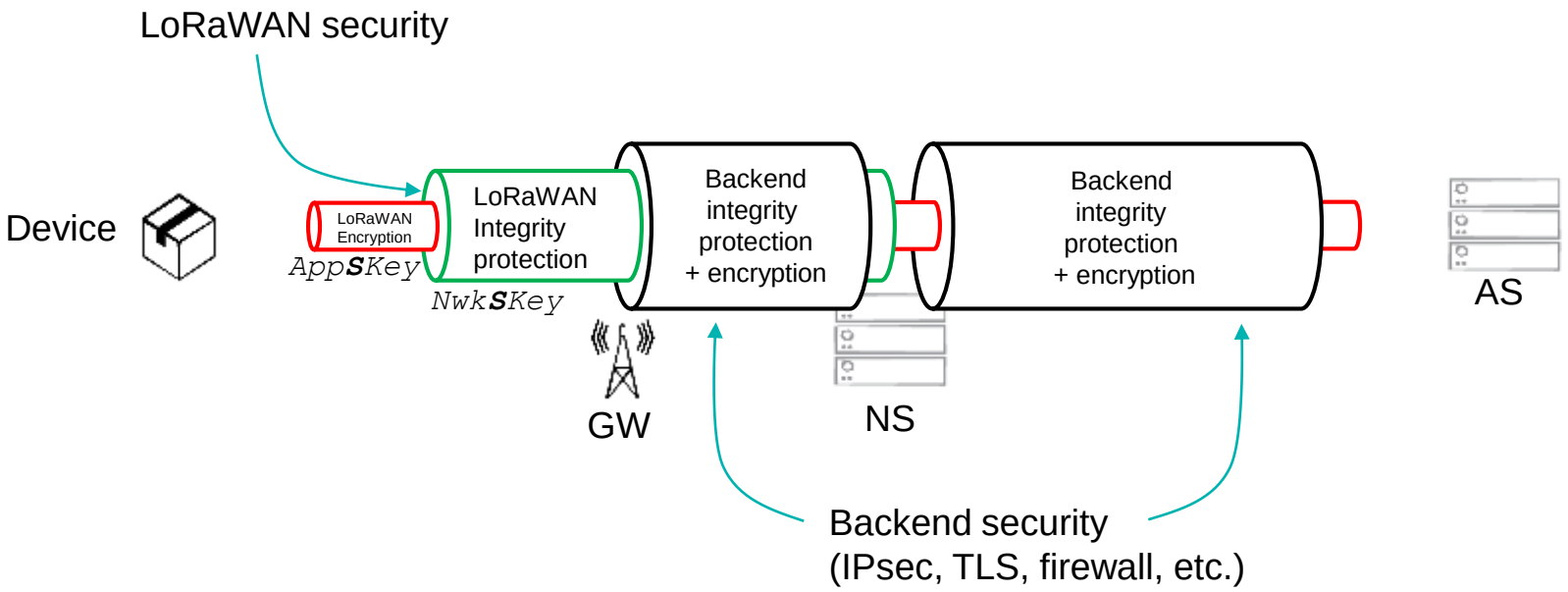
Payload Encryption + Data Origin Auth, Integrity/Replay Protection



MIC: Message Integrity Code
AES-CCM*: AES Counter with Cipher Block Chaining Message Authentication Code, * is for encryption-only variation defined in Zigbee standard

Actility

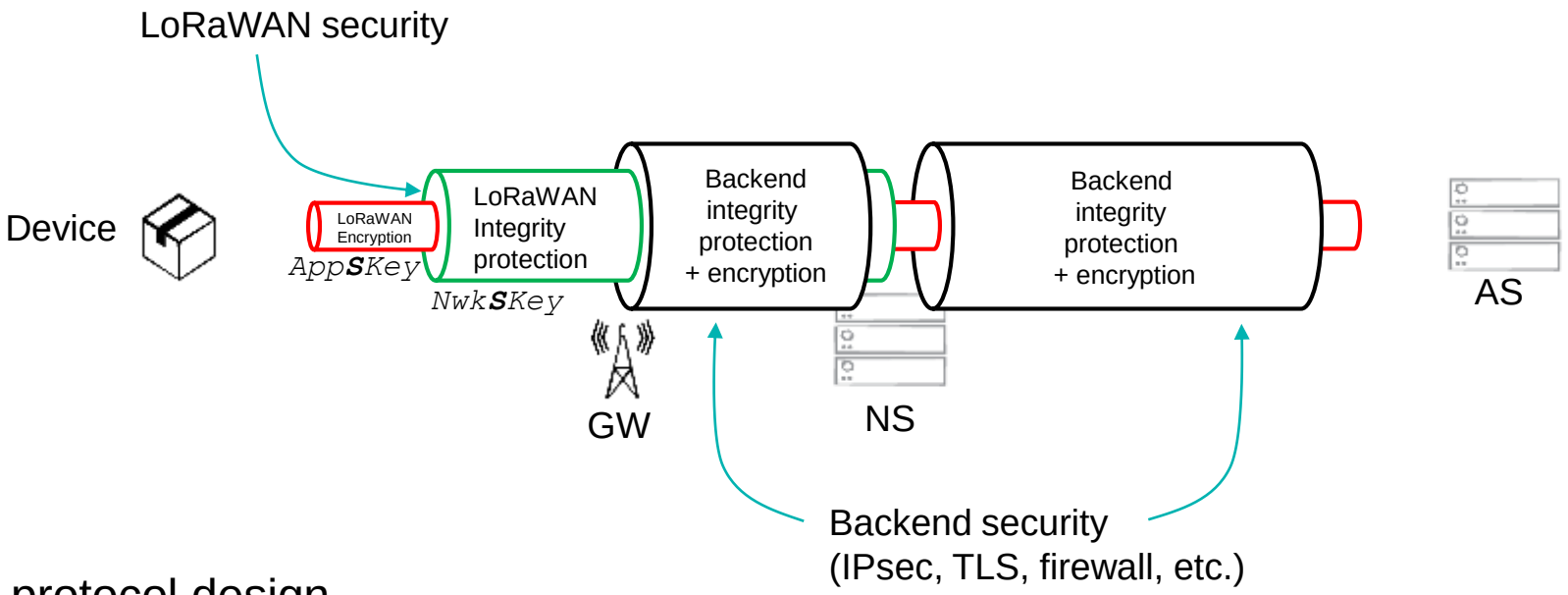
LoRaWAN End-to-end (Transport) Security



Note1 – "Integrity protection" represents "data origin authentication, integrity & replay protection"
Note2 – Supports encryption of MAC commands between the device and the NS
Note3 – Application-layer e2e integrity protection is left to the apps as an option

Actility

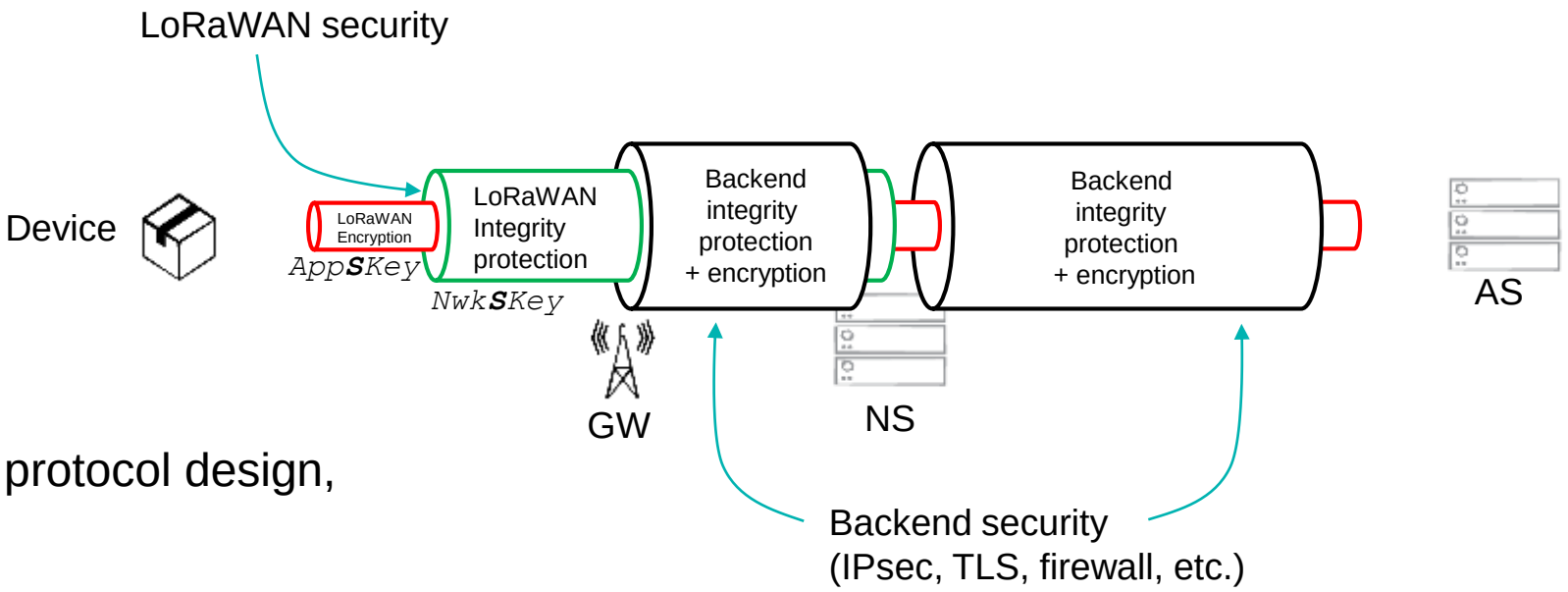
LoRaWAN End-to-end (Transport) Security



Communication protocol design.

Actility

Overall/Complete Security

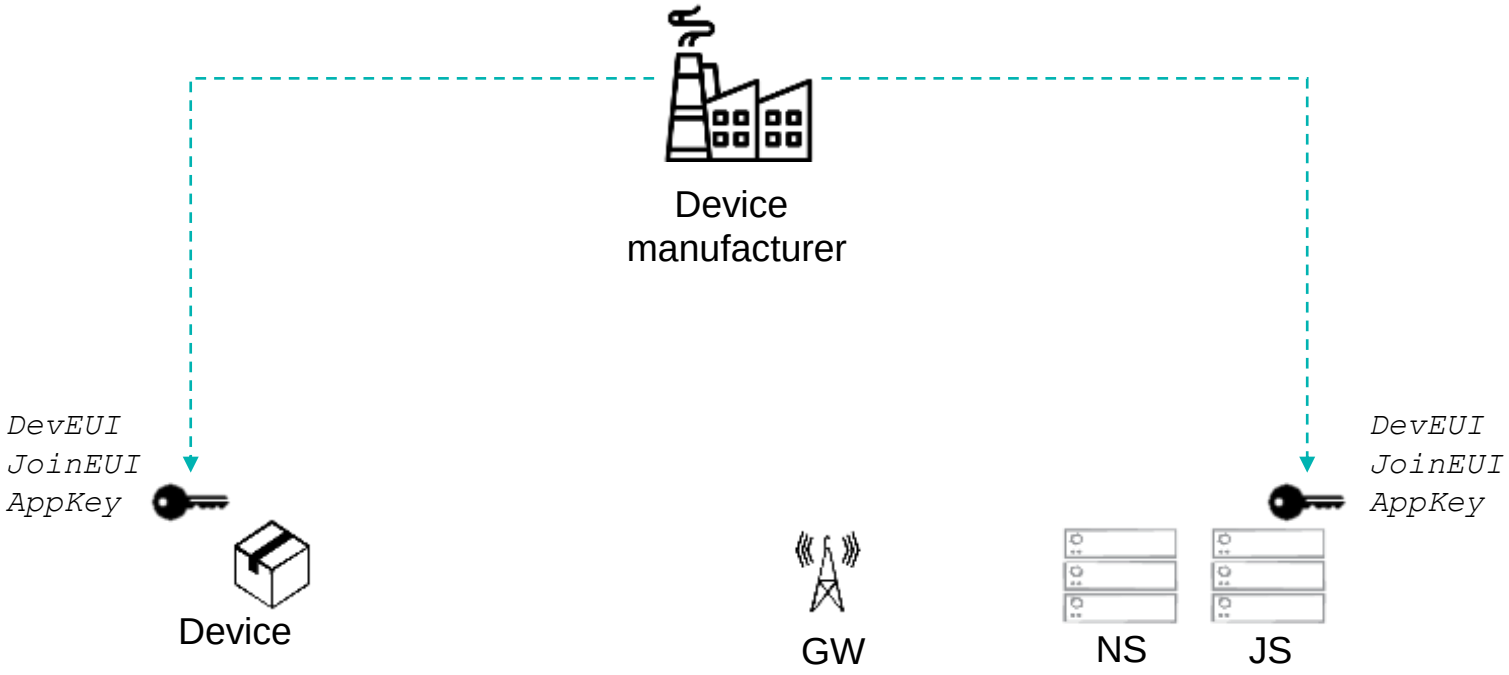


Communication protocol design,
implementation,
deployment.

Application security,
Device HW/SW platform security,
Infra platform security.

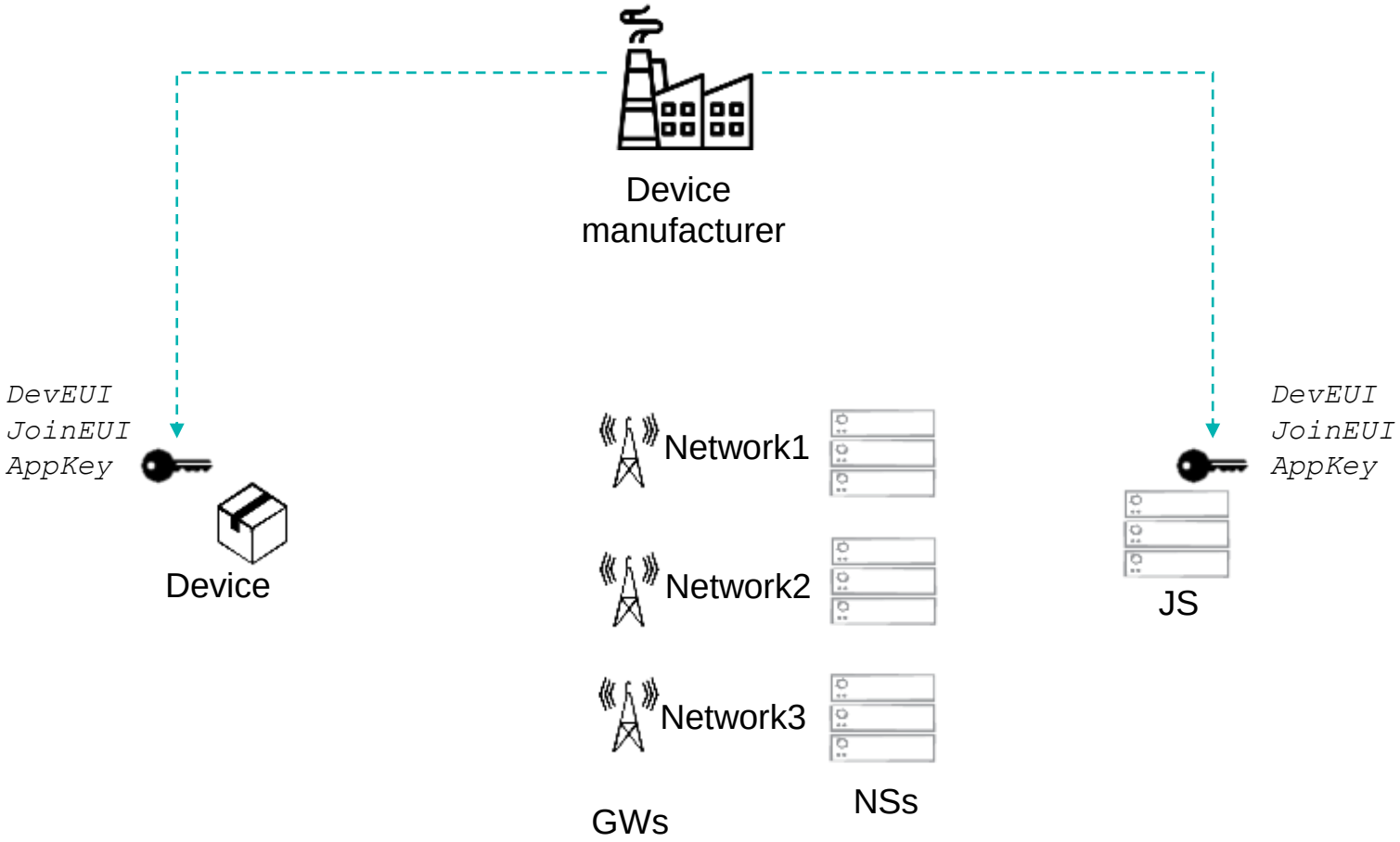
Actility

Device Provisioning



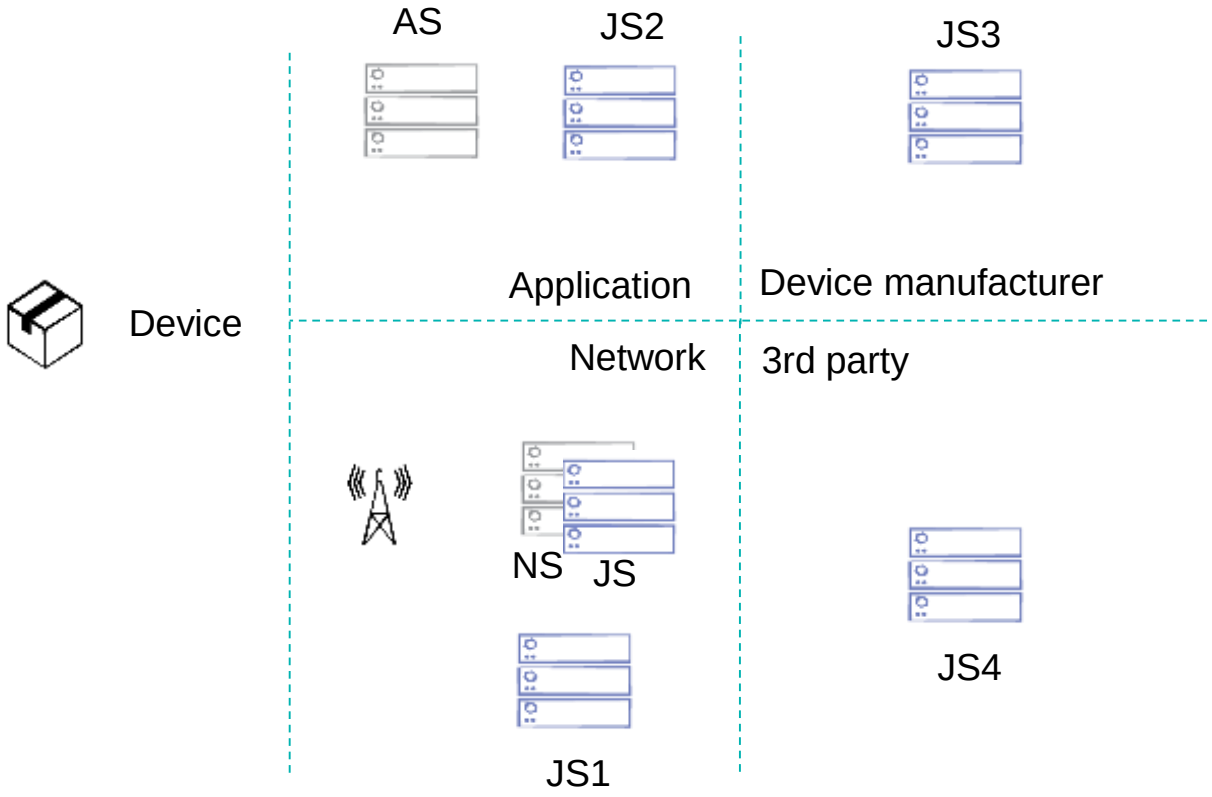
Actility

Network-agnostic Provisioning



Actility

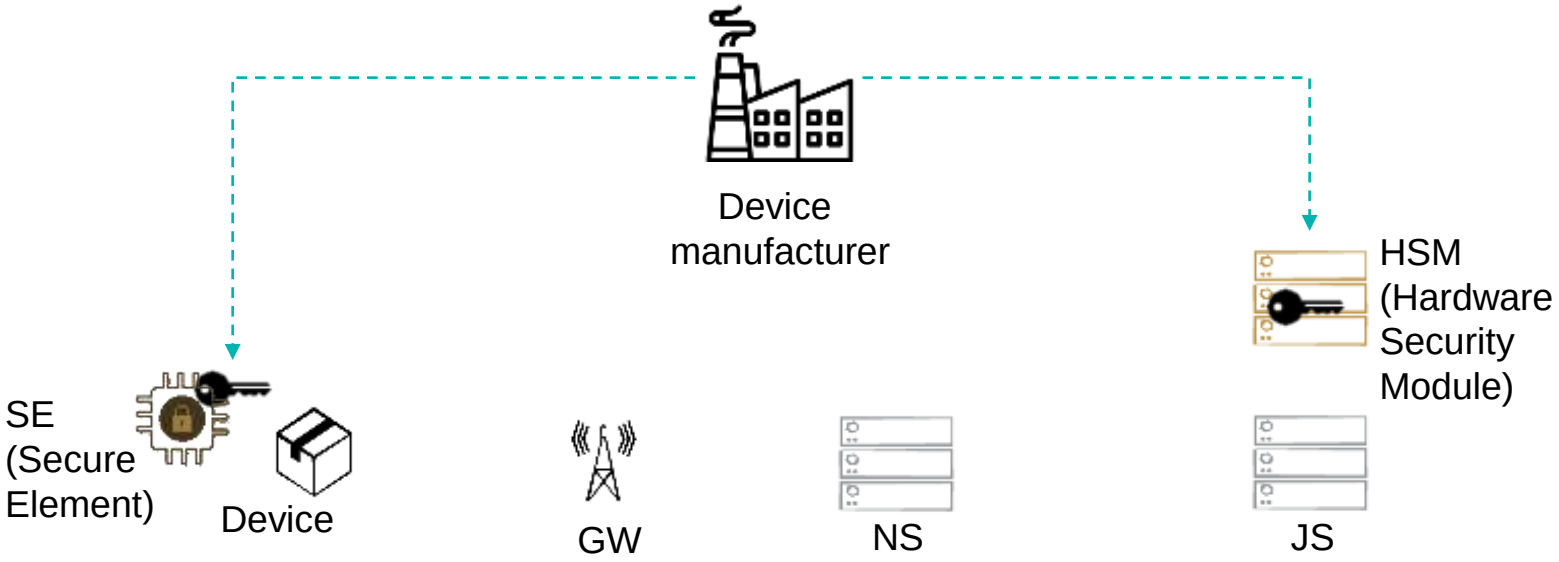
Deployment Flexibility



Various options for where the JS of a Device can be hosted

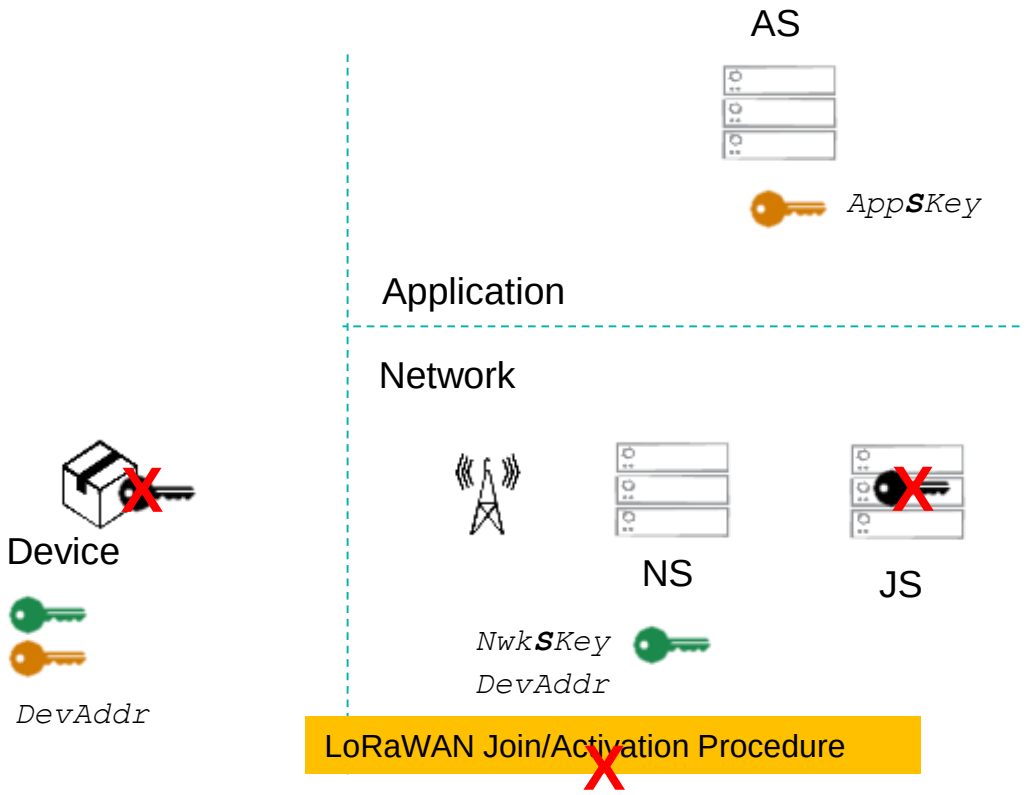
Actility

Hardware Security



Actility

OTAA vs ABP



OTAA (Over-the-Air Activation) dynamically generates session keys from root keys.

ABP (Activation by Personalization) devices are provisioned with session keys for ”a” pre-selected network.

Prefer OTAA because:

- ABP device can only work with a single network in its whole life
- ABP device cannot rekey sessions

Actility

LoRaWAN 1.1 Improvements

- Additional replay protection

32bit FCnt, disallow ABP FCnt reset, no DL retransmit, UL MIC bound to TxDr/TxCh, counter-based Join nonce values, Ack frame MIC uses Acked FCnt

- Separation of security realms

Distinct root keys and FCntDown for App and Nwk, UL MIC check in "stateful" visited network

- Enhanced key management

Richer key hierarchy with purpose-built session keys, re-keying w/o resetting data session

Actility

LoRaWAN 1.1 Improvements

- Additional replay protection

32bit FCnt, disallow ABP FCnt reset, no DL retransmit, UL MIC bound to TxDr/TxCh, **counter-based Join nonce values**, Ack frame MIC uses Acked FCnt

Applied to LoRaWAN 1.0.x: "Technical Recommendations for Preventing State Synchronization Issues around LoRaWAN™ 1.0.x Join Procedure"

- Separation of security realms

Distinct root keys and FCntDown for App and Nwk, UL MIC check in "stateful" visited network

- Enhanced key management

Richer key hierarchy with purpose-built session keys, re-keying w/o resetting data session

lora-alliance.org/resource-hub/technical-recommendations-preventing-state-synchronization-issues-around-lorawantm-10x

Actility

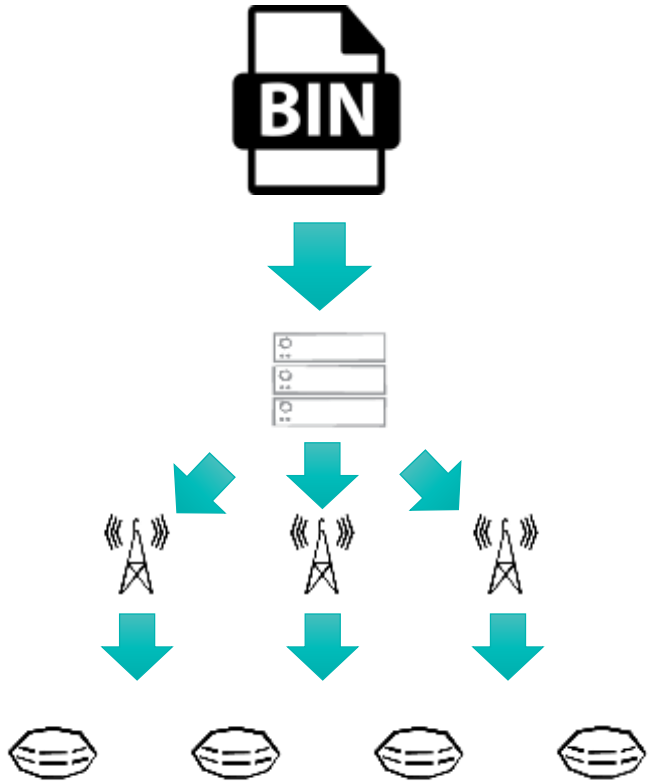
Firmware Update over the Air (FUOTA)

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

Actility

DOs and DONTs

- Pick secret keys randomly and per-device, deliver and store securely
- Don’t use arbitrary DevEUIs (respect IEEE OUIs)
- Don’t use arbitrary DevAddrs (respect LoRa Alliance NetID/NwkID allocations)
- Don’t use arbitrary JoinEUI/AppEUI (must point to a real JS with legitimate IEEE OUI)
- Use trusted OS/ HW security for sensitive apps
- Ensure end-to-end, whole-stack system security

- Contribute to Technical Committee
  - Finding issues & proposing solutions
  - On-going work
    - QR code for facilitating device provisioning
    - Over-the-air device personalization

```
DevEUI
JoinEUI
Mfr/Model
etc…
```

OUI: Organizationally Unique Identifier

Actility

Actility
Connecting with intelligence

- Leading LoRaWAN system vendor
  - Over half of national public networks globally powered by ThingPark platform
- Most comprehensive product/service portfolio
- LoRa Alliance leadership
  - Founding member, Alliance Vice-chair, Board Member, Technical Committee Co-chair, Developer Community WG Chair, and active across all groups
- Developer network
  - 1000+ registered members
- B2B marketplace
  - 150+ sellers

IoT connectivity platform

ThingParkWireless
Core network management solution For public IoT networks & service providers

ThingParkEnterprise
Powering IoT connectivity solutions dedicated to enterprise applications

ThingParkOS
IoT network business enabler

ThingParkX
Data analytics and control framework

IoT market enablers

ThingParkLocation
Geolocation and tracking of IoT devices

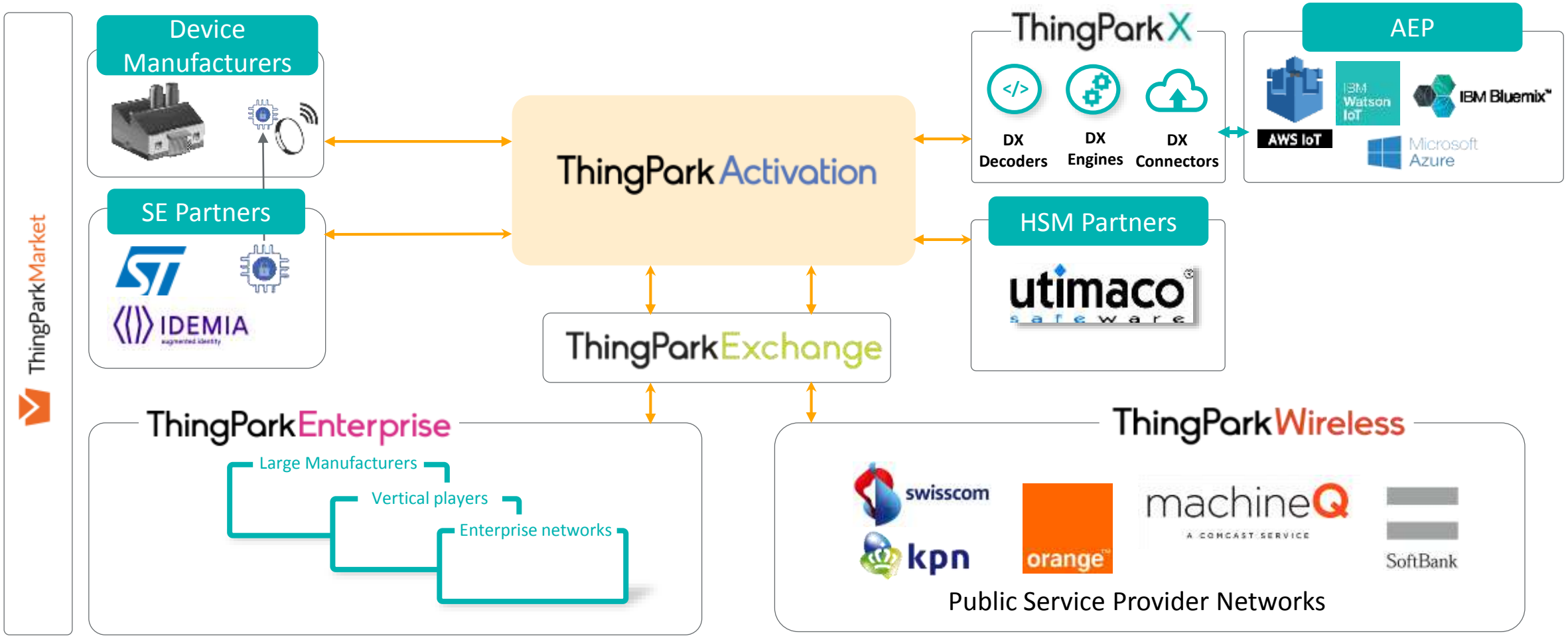
ThingParkEnergy
Smart grid, flexibility market & energy efficiency

IoT ecosystem digital services

ThingParkDevelopers
Developer support and go-to-market accelerator

ThingParkMarket
B2B e-commerce hub for IoT

ThingPark and Security



ThingPark Activation webinar: www.youtube.com/watch?v=mZgTr5VZiuI
Roaming/ThingPark Exchange webinar: www.youtube.com/watch?v=tWP6VV1CKEg

Actility

Questions?

www.actility.com

Actility