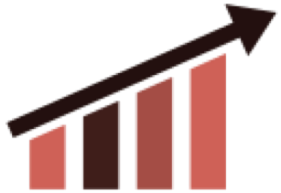
Actility
Connecting with intelligence

LoRaWAN Device Activation Webinar

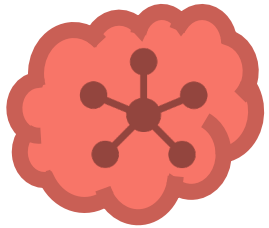
13th of September, 2018

Implementing a secure & streamlined Device Activation process is a real challenge

End-to-end security



Scalable process



Global Roaming

As a device owner...

- Ensure the confidentiality of my sensor's data up to the Application platform
- Secure device ownership so nobody else can use it
- Benefit from an easy device activation on any LoRaWAN network

As a device manufacturer...

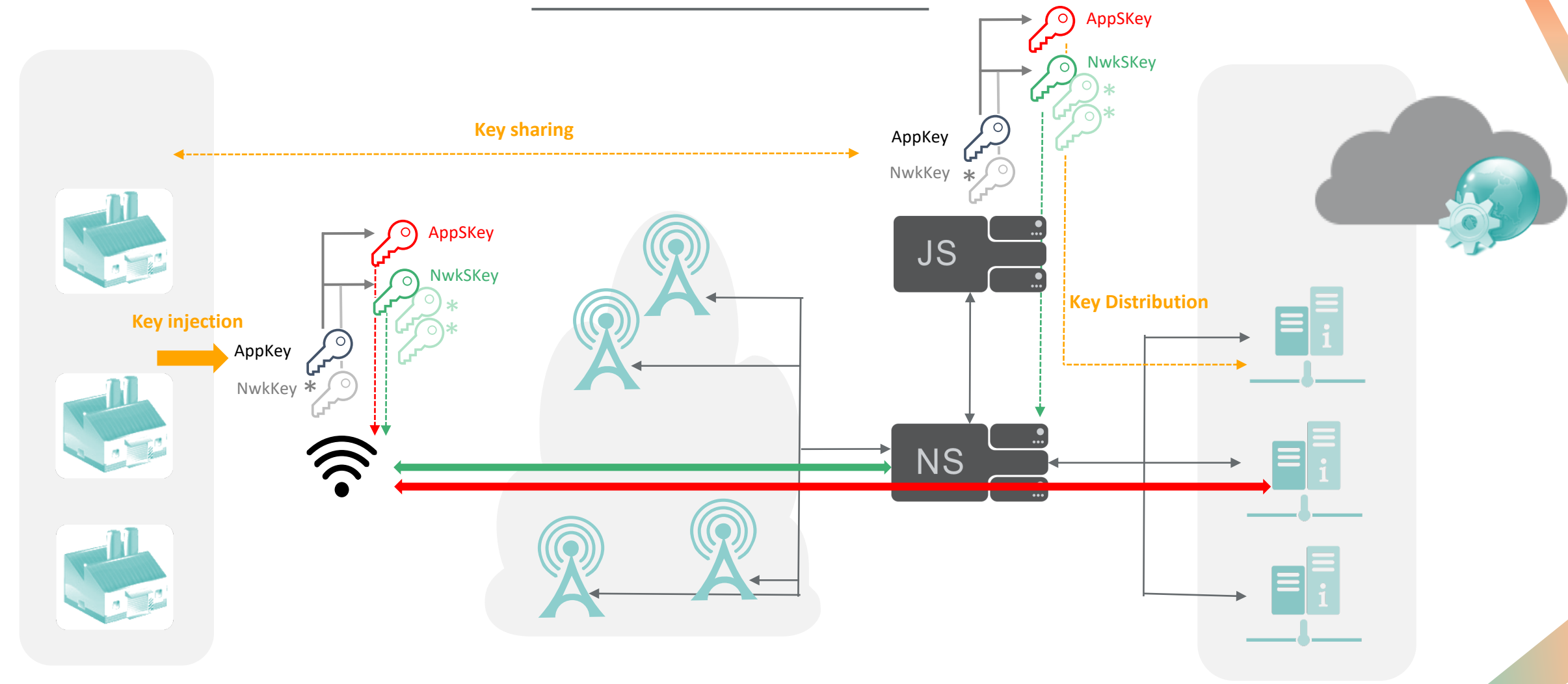
- Implement a generic manufacturing process with personalization independent from network operator
- Ensure security secrets are shared only with necessary parties
- Sell ready-to-use products with no complex on-boarding procedure for multiple network operator or application platform providers

As a LoRaWAN service provider...

- Implement a simple on-boarding process for a wide portfolio of devices
- Deliver the right level of security according user's expectations and use cases

Actility

LoRaWAN™ Security Overview



Actility

From the factory to the network...

... 3 steps to device activation

Device Personalization

- Inject keys during production
- Ideally, inject in Join Server at same time by same key holder
- Ideally, generic personalization (AppEUI)

Device Maker

AppKey
DevEUI
AppEUI

Device Commissioning

- Device sold to Subscriber with home network Connectivity Plan
- Device associated to Connectivity Subscriber account on home network

Network Operator

SubscriberID
Device Profile
Service Profile
Routing Profile

Device Activation

- Device is powered on, from home or away from home
- Join_Req is sent on visited network, and routed to Join Server

JOIN

DevAddr
AppSKey
NwkSKey

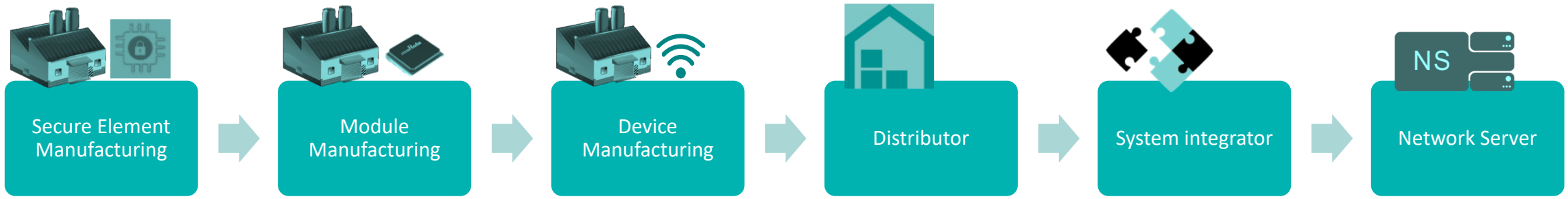
Challenges

- Share keys to Join Server with minimum exposure
- Personalize device so it points to correct Join Server (AppEUI/JoinEUI selection)

Actility

The AppKey sharing challenge

Keys should never be transferred in clear – ensuring security over a long chain of custodians is very complex



Optimal flow is to only share secrets between key holder and Join Server

ThingPark Activation

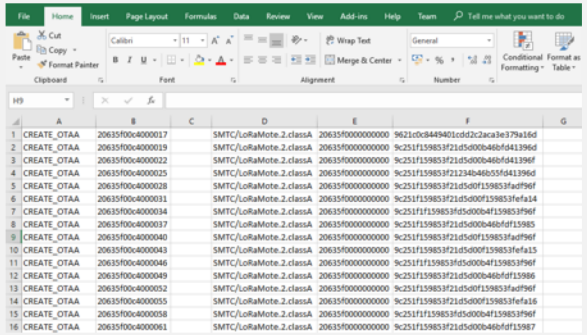
Actility

How are people sharing AppKey today

Written on back of device

- Low security
- Error prone
- Complexity increase with scaling

Encrypted CSV



- Low security (all data in clear once file is open)
- Need to split the file as devices are bought by different parties
- Complexity increase with scaling

Web service and storage

- Another party in the chain: another account, another process
- Connectivity to other systems is proprietary
- Cost of securing additional server

Security issue / Scalability issue

Actility

The AppEUI selection challenge

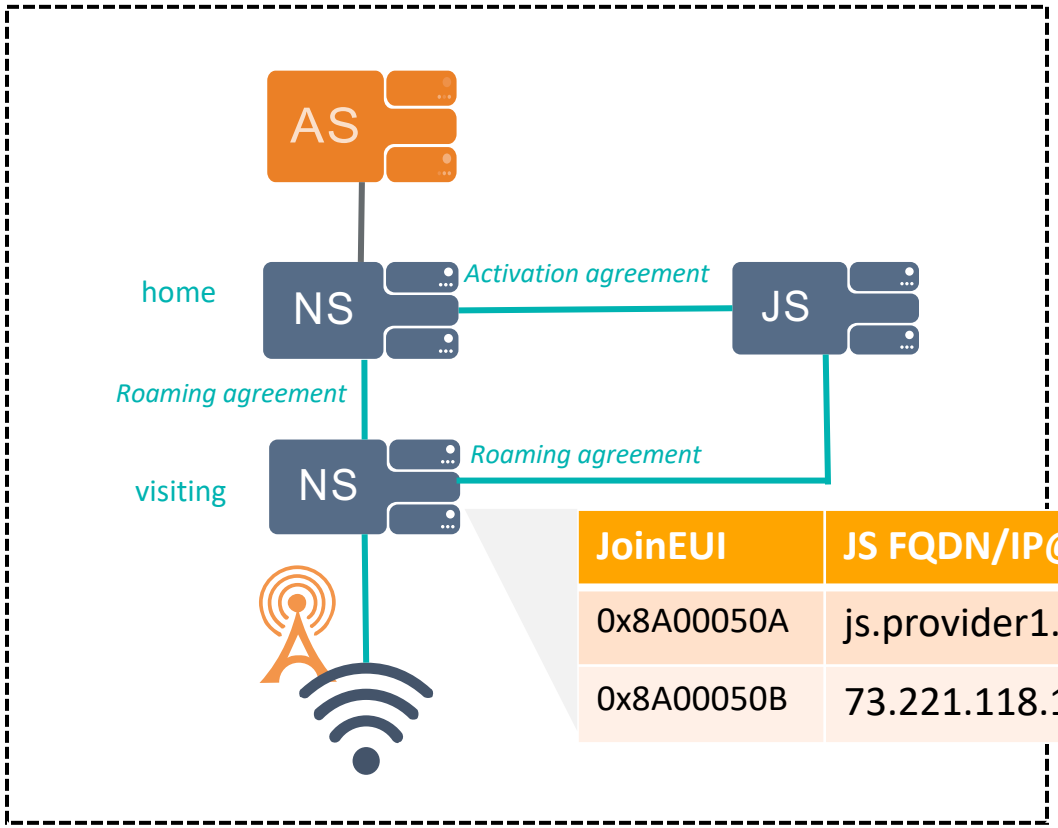
Application	Connectivity	Security
		
Application Server ➢ Control your IoT application ➢ Data processing once available on the platform ➢ Mostly selected by Device Manufacturer today	Network Server ➢ LoRaWAN connectivity provider ➢ Retrieve data from devices over wireless interface ➢ Selected by System Integrator or End User	Join Server ➢ LoRaWAN security provider ➢ Handle secret keys and send temporary session keys to other servers ➢ Who and how to select it?
Application Subscriber account	Connectivity Subscriber account	Security Subscriber account

An IoT connected device and its application may have multiple homes with multiple accounts

Actility

AppEUI and Join Server binding

Passive Roaming



JoinEUI	JS FQDN/IP@
0x8A00050A	js.provider1.com
0x8A00050B	73.221.118.14

- AppEUI/JoinEUI must be selected during device personalisation
- Activation at home
  - hNS must have business agreement with JS
  - Possible to route all JoinEUI to same pre-defined JS
- Activation away from home
  - s/fNS must have business agreement with JS
  - s/fNS must share security credentials with JS
  - s/fNS must be able to translate JoinEUI⟷JS address to route JOIN procedure

Using arbitrary AppEUI/JoinEUI forbids any type of roaming

Actility

Who are the Join Server suppliers?

AppEUI/JoinEUI
AppKey

Connectivity supplier

- Bundled connectivity and security
- Requires a dedicated device batch per connectivity supplier
- Or re-personalisation is needed and secret keys must be shared until the end user

Pure security suppliers (Trusted Key Manager)

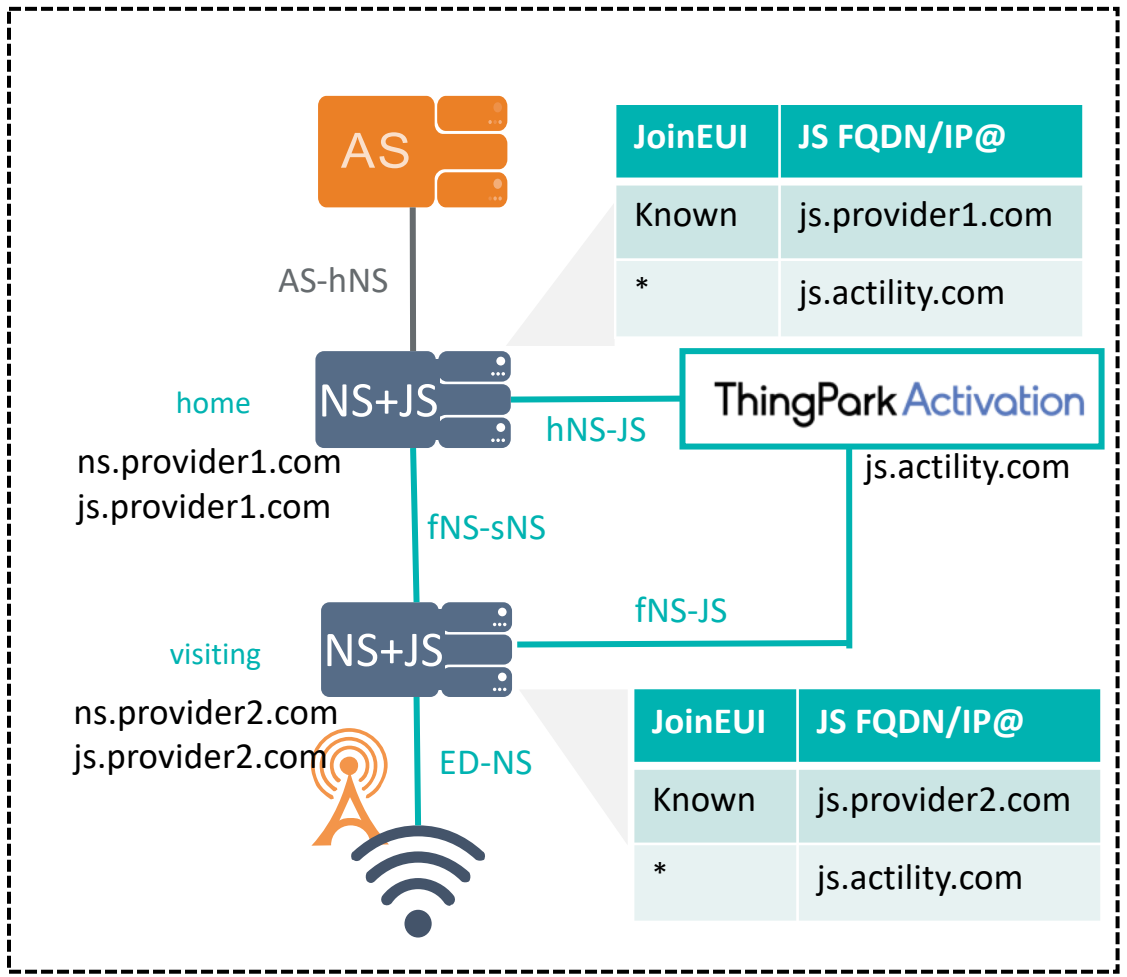
- Often bundled with dedicated hardware (Secure Element)
- Requires (home) interconnection with all connectivity suppliers
- Requires activation agreements with all connectivity suppliers

A Join and Roaming Service supplier

- Focused on simplifying the provisioning workflow amongst all parties
- Naturally interconnected and roaming with all connectivity supplier
- Onboard multiple security partners

Actility

Possible implementation with arbitrary AppEUI allocation



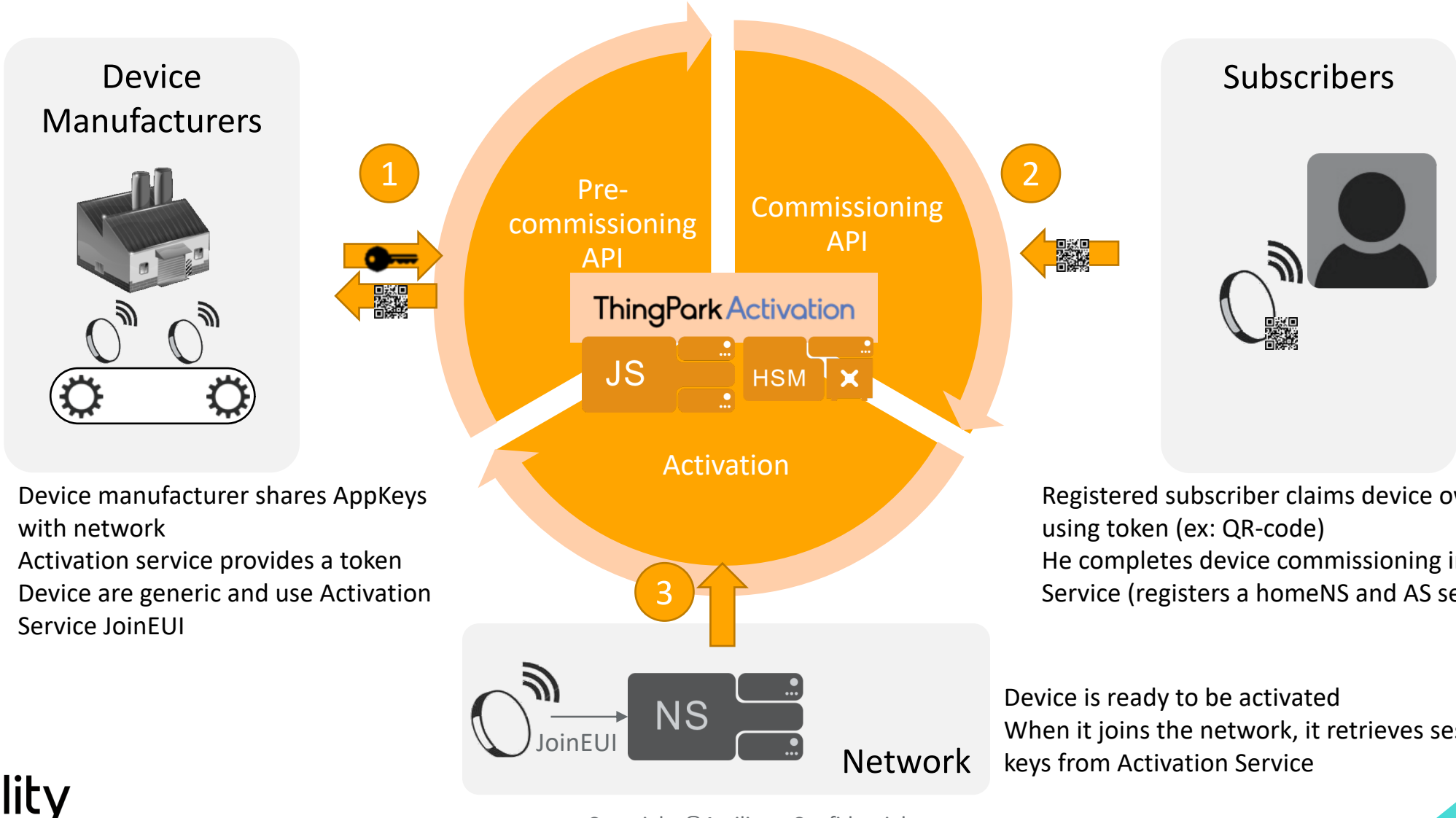
Legacy devices with arbitrary AppEUI / JoinEUI can be enabled for roaming as follow:

- Setup hNS to route all home traffic (provisioned devices) to home JS
- For visited network, setup fNS to handle known home traffic (provisioned devices) locally, and route all unknown traffic to a unique JS

- **Actility implementation**: ThingPark Activation allows to deal with all devices which are not known by visited NS
  - ⇨ Home unknown roaming devices in central JS

Actility

ThingPark Activation Service workflow



Device manufacturer shares AppKeys with network
Activation service provides a token
Device are generic and use Activation Service JoinEUI

Registered subscriber claims device ownership using token (ex: QR-code)
He completes device commissioning in Activation Service (registers a homeNS and AS security)

Device is ready to be activated
When it joins the network, it retrieves session keys from Activation Service

Actility

Actility Secure Element (SE) partnership

ThingPark Activation

SECURE ELEMENT PARTNERS

- ✓ Guarantee security on device side
- ✓ Simplifying commissioning process

Actility partnership with SE vendors helps Device Manufacturers:

1. Secure storage of AppKeys for High Security Use Cases
2. Protocol stack uses AppSKey without having access to it (hence neither attackers)
3. Device Manufacturer don't need to generate and distribute AppKeys, this is already done between SE manufacturer and ThingPark Activation Service
4. If personalized SE are ordered (with dedicated DevEUI block), Device Manufacturer needs no LoRaWAN™ personalization: simply solder the SE.

End-to-end data security and device onboarding is mostly handled between Actility and SE partners

ThingPark Activation is secured with Hardware Security Modules

ThingPark Activation runs with HSM in SaaS

No compromise on security and availability

- 2 HSMs for high availability and geographical redundancy
- Appliance cost is shared between SaaS users

Fully secured AppKey

- Full integration of LoRaWAN code inside the HSM so keys never leave the HSM
- Support LoRaWAN 1.0 and 1.1 devices

Simplified provisioning when using Secure Element

- Secrets can be shared with Secure Element partners in a trusted environment
- Full integration with security partners allows simpler provisioning flows with no key sharing

utimaco® safeware

Leader in Certified HSMs for Smart Metering

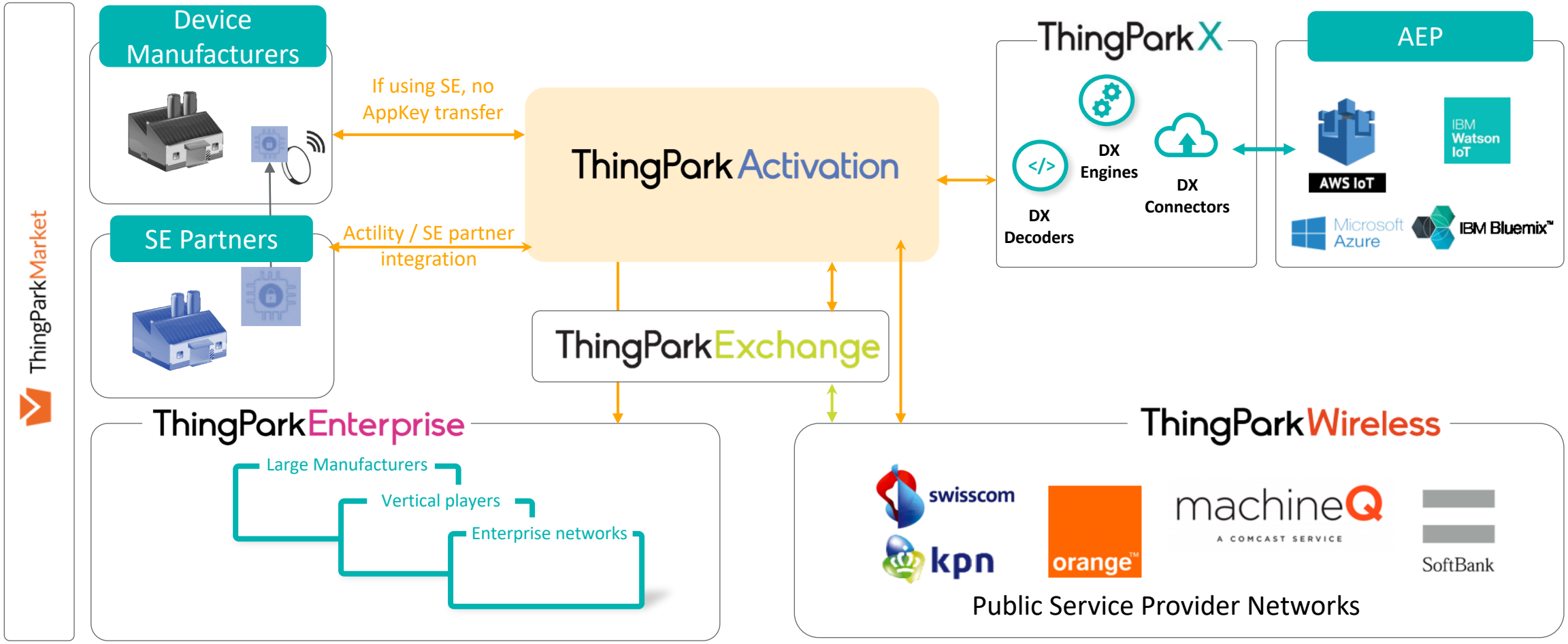
CryptoServer SE series

Utimaco SE52

- *Standard HSM*
- *Tamper resistant technology*
- *Certified FIPS 140-2 Level 3*
- *Secure key storage and processing*
- *SmartCard for strong authentication*
- *Separation of duties*
- *Remote Management*

Actility

Actility ecosystem



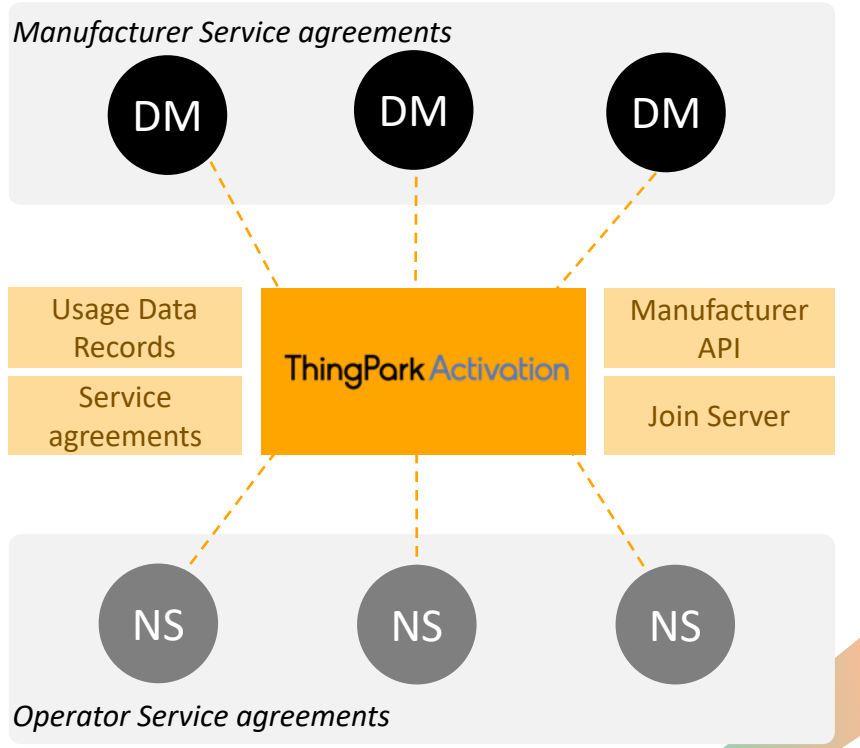
More about ThingParkExchange (Actility advanced roaming hub): https://www.youtube.com/watch?v=tWP6VV1CKEg

Actility

ThingPark Activation Service Value Proposal

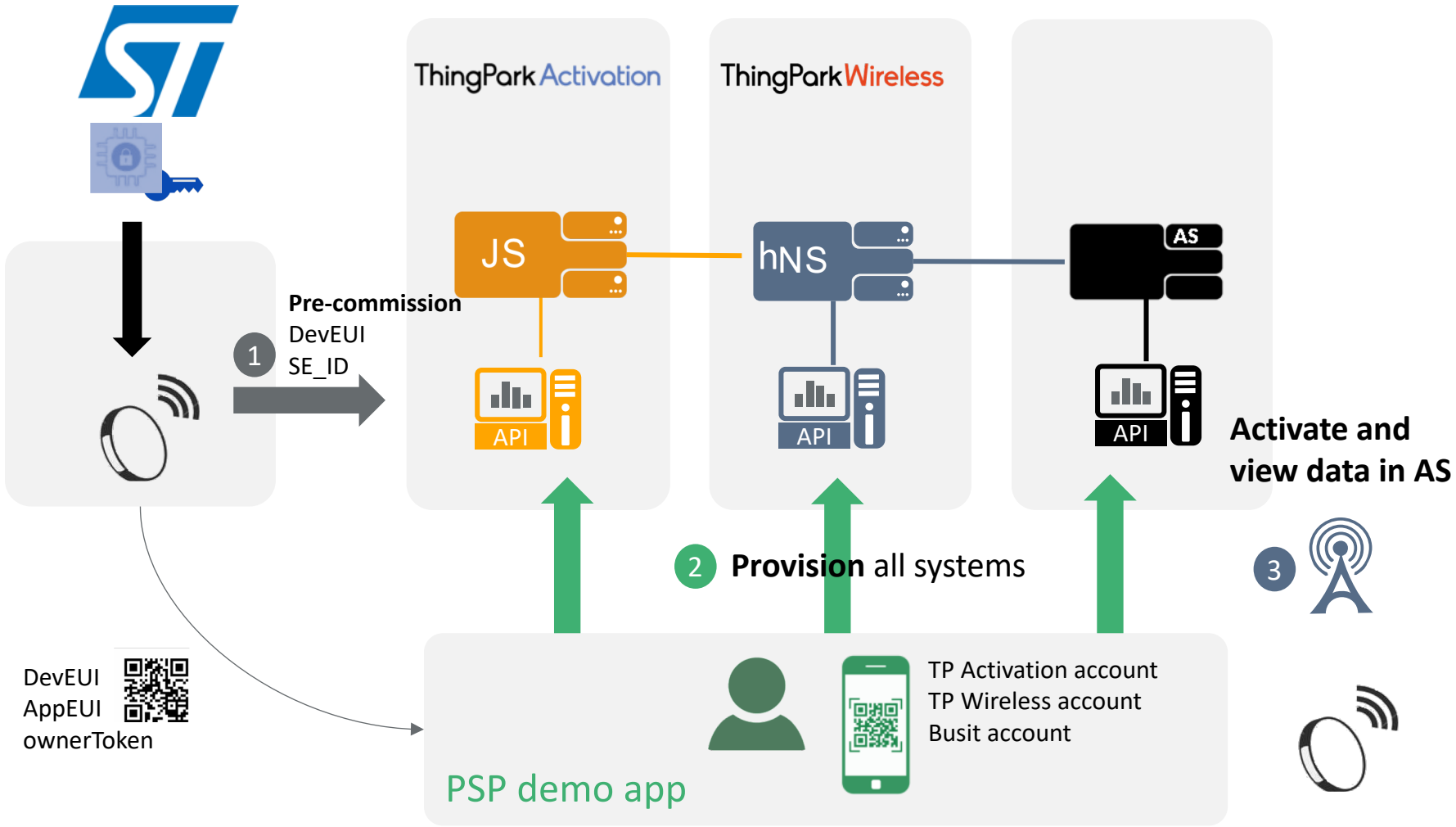
Simplified device activation for all onboarded Service Providers and Device Manufacturers

- **Truly generic device production**: Unique (set of) JoinEUI(s)
- **Reduced operational cost for device activation**: no secure key transfers
- **Focus on connectivity**: rely on **Trusted Service** for security audits
- **Activation Service with SE and HSM options**: Highend Security use cases at optimised cost
- **Future proof service**: **Roaming services**, early availability of LoRaWAN 1.1 support and upcoming Alliance items



Actility

ThingPark Activation Integration demo



Actility

How to onboard ThingPark Activation

Contact your Actility sales representative for more information on

- ThingPark Activation onboarded ecosystem
- ThingPark Activation coming POCs and demos
- ThingPark Activation price list

For all technical enquiries: norbert.herbert@actility.com

Actility

Q&A

Actility