Simplifying Device Deployments with Generic Secure Element and Bootstrapping Join Service

Actility & IDEMIA

Not to be shared without prior consent by the LoRa Alliance®
Generic Secure Element and Bootstrapping Join Service
LoRaWAN® Security Overview

Device Manufacturers → End Device (ED) → Gateways (GW) → Join Server → Network Server → Application Servers (AS)

Key injection: AppKey, NwkKey

Key sharing: AppSKey, NwkSKey

Key Distribution:
- AppKey
- NwkSKey
- AppSKey
- NwkKey

Creating Valuable IoT Connections | lora-alliance.org
LoRaWAN® Device Deployment

LoRaWAN® defines cryptographic primitives used for security

- Authentication with MIC/NwkSkey
- Confidentiality with AppSKey encryption
- Session key generation based on AppKey during Join procedure
- Session key distribution based on LoRaWAN® backend interface

However, LoRaWAN does not define the Secret Key handling

- AppKey injection
- AppKey sharing

Coming from smart card industry, we have defined a secure way of personalizing secure element for LoRaWAN
Secret Key Handling, a Primer

1. A secret key value is never exposed!
2. A secret key is handled inside a Hardware Security Module (HSM) in a High Security Area (HSA)
3. A secret key is under the responsibility of its owner, i.e. not shared 😊

In a physical world …

The owner of the key can open the safe …

In a digital world …

When a key is transferred, the key is duplicated.

See point 3 above…

Certified tamper resistant hardware appliance handling cryptographic functions and storage

Certified security area with physical barriers, access control and surveillance made available on a secured network
Secure credentials provisioning

Bootstrap credentials (DevEUI, JoinEUI, AppKey) are securely provisioned in the Secure Element from a HSA (High Security Area)

- No End-Device personalization required
- Simply solder Secure Element

Bootstrap credentials are also securely transferred to an Identity Management System (IDMgr)

- Manage Secure Element life cycle: Initial Join, reprovisioning services, Fleet Transfer, Key renewal …

Bootstrap secret keys are never exposed
Re-Personalization over the air

1. End-Device joins via a bootstrap network using IDMgr
   - Using LoRaWAN® L2 and backend interface
   - Secure Element bootstrap credentials are known to IDMgr

2. IDMgr sends customer profile to Secure Element
   - Using End-Device application layer
   - Customer profile is sent over the air, including encrypted AppKey, secured via Message Layer Security protocol in Secure Element

3. End-Device re-joins via customer network
   - Using LoRaWAN® L2 and backend interface
   - Customer network is provisioned with final credentials
Use a peering hub to facilitate interconnection

IDMgr is connected to bootstrap JS but not necessarily to customer JS
- Select a JS supplier: operator, manufacturer or JSaaS

IDMgr is connected to bootstrap NS
- Select a bootstrap network supplier
- It should ensure bootstrap coverage via roaming agreements
Benefits of bootstrapping & OTA re-personalisation

- Generic Secure Element
- Over-the-air profile delivery

- Extensible Application layer
- Independent from LoRaWAN® MAC version

- Isolation of security domains across all instances of JSs
- ID manager can be operated by separate supplier

Generic and secure devices ready to be activated on all LoRaWAN® networks
Come and see our demo at Actility’s booth
Actility ThingPark Activation Service

**Generic device onboarding**
- Solder IDEMIA Secure Element to onboard ThingPark Activation
- Device manufacturer benefits from unique Activation agreement for all onboarded operators
- Can be used in parallel with existing Activation agreements (i.e. other Join Servers)

**Operators can onboard massively**
- All onboarded device manufacturers can join the Operator network
- Service secured with Hardware Security Module (HSM)
- Supports Passive Roaming Activation, using direct or hub roaming connectivity
IDEelia M-TRUST Security Services

Generic device onboarding
- Solder IDEelia Secure Element to onboard ThingPark Activation
- In field re-provisioning service to final destination

Security services
- Support in field migration use cases
  - Fleet ownership, NS/JS change
- Support key renewal upon security policy
- Support secure command use case
- Support custom security services
Q&A session

THANK YOU

Not to be shared without prior consent by the LoRa Alliance®