

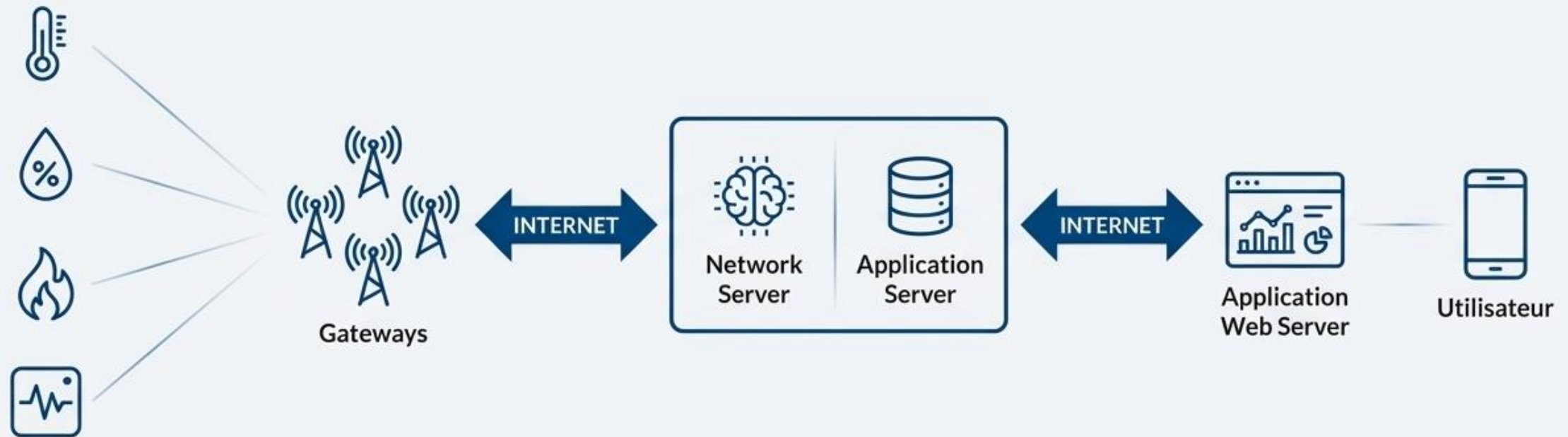
Le Voyage d'une Donnée à travers l'Architecture LoRaWAN

De la genèse du capteur à l'application finale, une exploration de bout en bout.



L'Écosystème LoRaWAN : La Carte du Voyage

LoRaWAN est le protocole qui orchestre la communication sur la chaîne complète : du Device au serveur d'application. Il s'appuie sur la modulation LoRa pour la transmission radio.



LoRa

La modulation physique entre le device et la gateway.

LoRaWAN

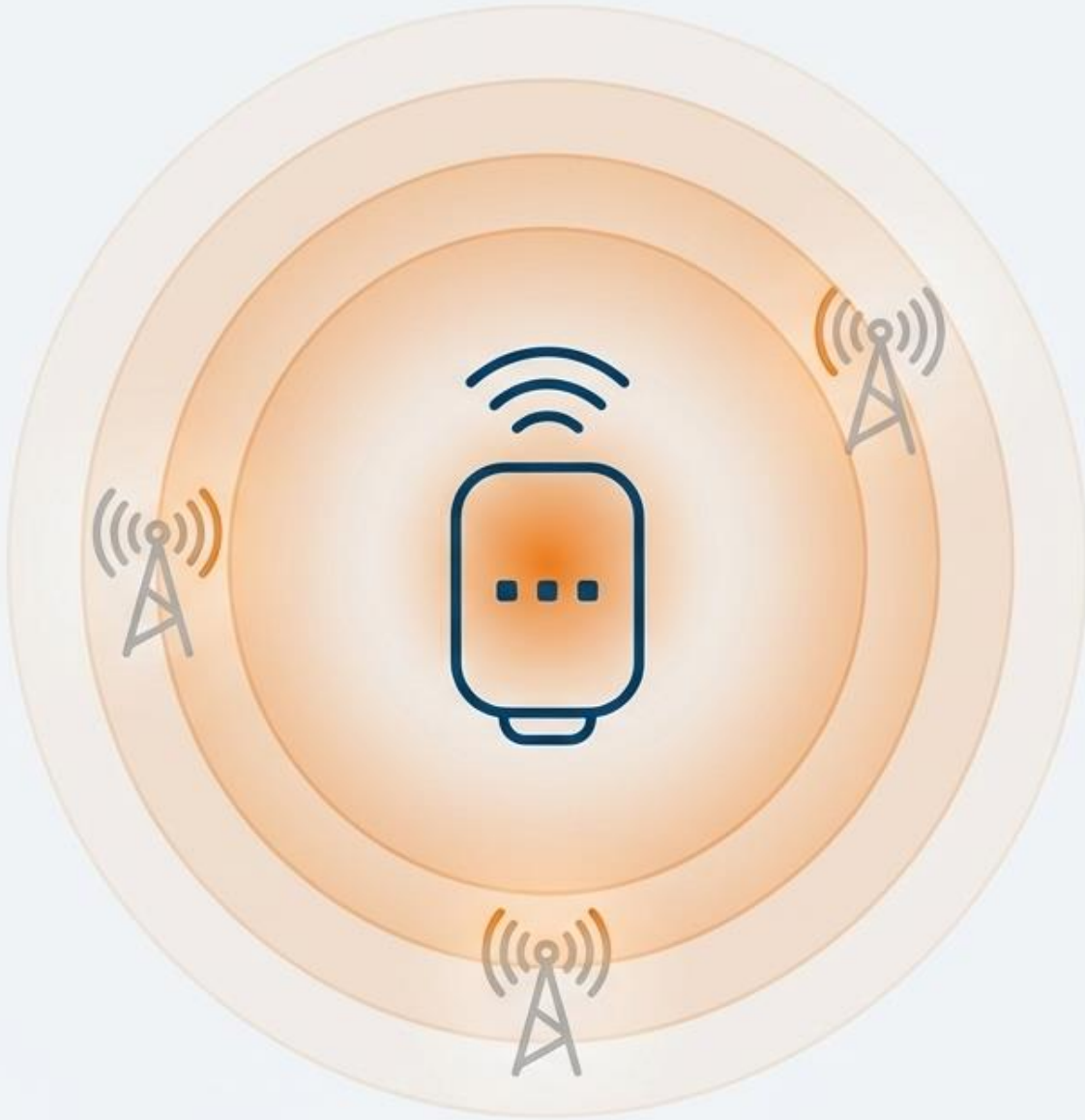
Le protocole réseau qui gère la communication sur l'ensemble de la chaîne.

Le Point de Départ : Le Device LoRa

- Les **Devices LoRa** sont des objets connectés (IoT) qui collectent des données (température, humidité, etc.).
- Équipés d'une radio LoRa, ils diffusent leurs messages.

Point Crucial

Ils n'adressent pas une gateway spécifique. Toutes les gateways à portée reçoivent le message, assurant la redondance et la robustesse du réseau.



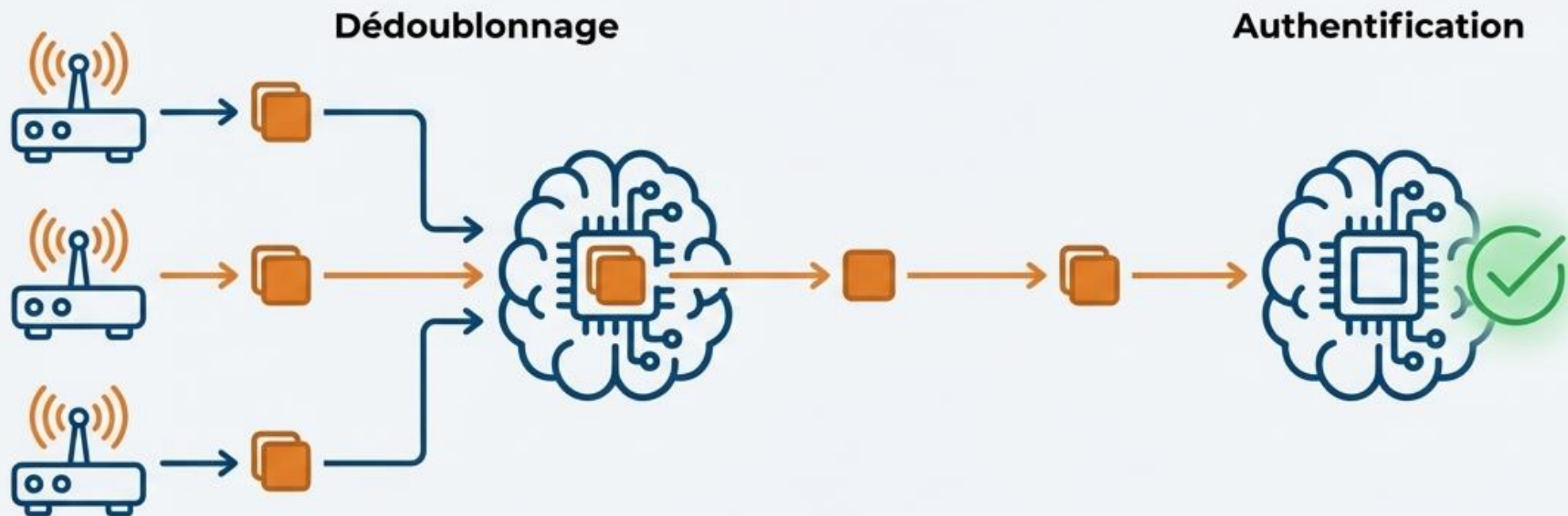
Le Premier Relais : La Gateway



- La Gateway joue le rôle de passerelle entre la modulation LoRa et une communication IP (Internet).
- Elle écoute en permanence sur tous les canaux et tous les 'Spreading Factors'.
- Lorsqu'elle reçoit une trame LoRa, elle la transmet via Internet au Network Server préconfiguré.
- Chaque gateway possède un identifiant unique (EUI) sur 64 bits.

Le Cerveau du Réseau : Le Network Server

Le **Network Server** centralise les messages reçus de toutes les Gateways.



Fonction 1 : Dédoublement

Il supprime les messages en double si plusieurs gateways ont reçu la même transmission.

Fonction 2 : Authentification

Il vérifie l'identité du Device LoRa pour s'assurer qu'il est autorisé à communiquer sur le réseau.

La Destination des Données : L'Application Server

- Souvent hébergé avec le Network Server, il gère la logique applicative.
- Il dissocie les applications les unes des autres : chaque application ne voit que les données des devices qui lui sont attribués.

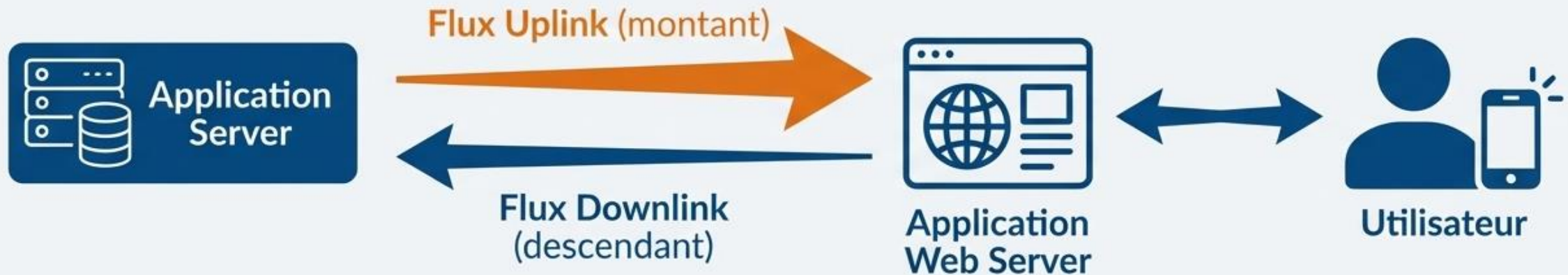
****Rôle principal****

Il déchiffre la charge utile des données (le 'Frame Payload') pour la rendre lisible.



L'Interface Utilisateur : Le Serveur Web Applicatif

Le serveur web applicatif met les données à la disposition des utilisateurs finaux (graphiques, tableaux de bord, bases de données).



Flux Uplink (montant)

Le flux principal dans l'IoT. Les données sont émises par les objets vers le serveur.

Flux Downlink (descendant)

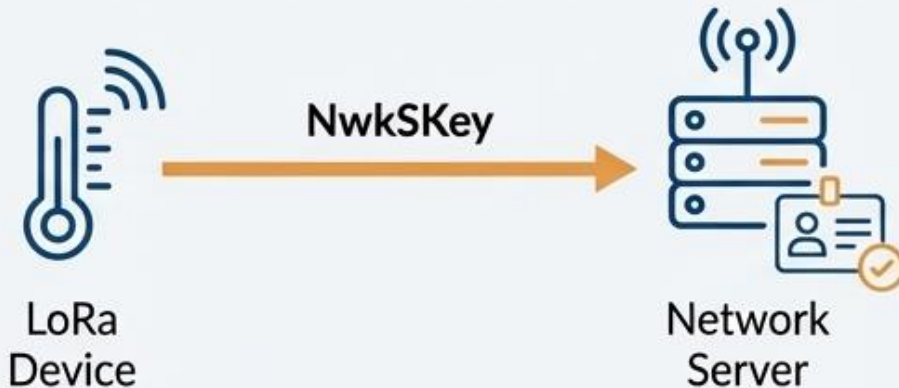
Il est également possible d'envoyer des commandes depuis l'application vers les Devices LoRa.

Sécuriser le Voyage : Les Deux Clés de la Confiance

L'architecture LoRaWAN utilise deux clés de session AES-128 bits distinctes pour garantir à la fois l'intégrité du réseau et la confidentialité des données.

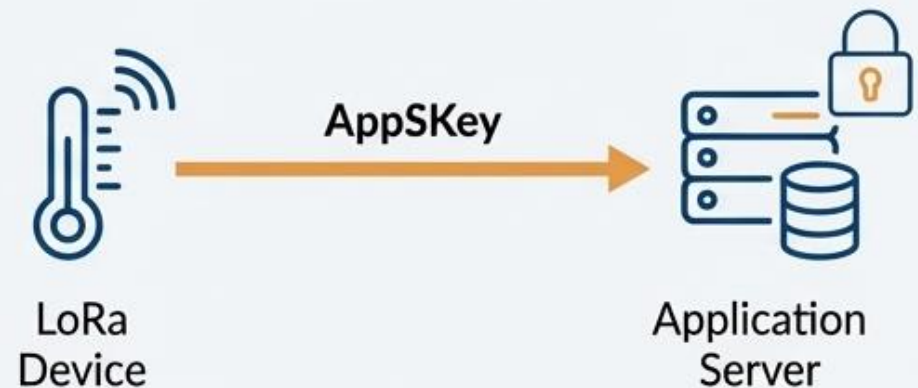
Network Session Key (NwkSKey)

Sert à l'**authentification** entre le Device et le Network Server. Prouve que le message vient bien d'un appareil autorisé.



Application Session Key (AppSKey)

Sert au **chiffrement** de bout-en-bout entre le Device et l'Application Server. Garantit que seul le destinataire final peut lire les données.



La Clé du Réseau (NwkSKey) : Le Laissez-passer

La **Network Session Key (NwkSKey)** est partagée uniquement entre le Device LoRa et le Network Server.

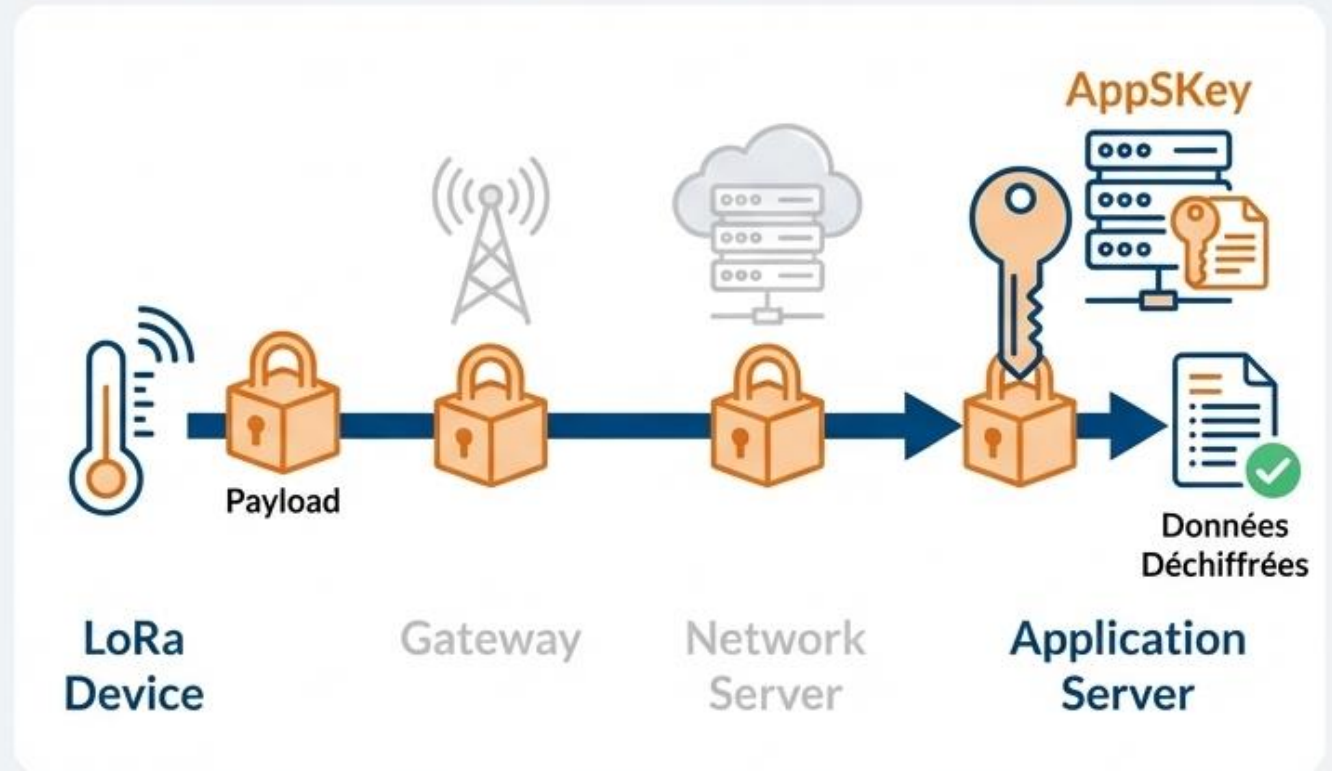
Elle garantit l'**authenticité** et l'**intégrité** du message. Le serveur peut être certain de l'origine du message et qu'il n'a pas été altéré.

Il s'agit bien d'**authentification**, et non de chiffrement de la donnée elle-même. La Gateway et l'Application Server n'ont pas connaissance de cette clé.



La Clé Applicative (AppSKey) : Le Sceau du Secret

- L'**Application Session Key** (AppSKey) est partagée de bout-en-bout, uniquement entre le Device LoRa et l'Application Server.
- Elle est utilisée pour **chiffrer** et **déchiffrer** la charge utile du message (le "Frame Payload").
- Ni la Gateway, ni même le Network Server ne peuvent lire les données du capteur. Cela garantit une **confidentialité** totale.



Chiffrement de bout-en-bout: Confidentialité garantie du capteur à l'application.

Le Point de Départ du Voyage : L'Activation

Pour communiquer sur le réseau LoRaWAN, un device a besoin de trois informations essentielles :



DevAddr

Un identifiant unique sur le réseau.



NwkSKey

La clé pour l'authentification.



AppSKey

La clé pour le chiffrement.

Il existe deux méthodes pour fournir ces informations au Device et au Serveur.



Activation By Personalization (ABP)

Les clés sont pré-programmées en dur.

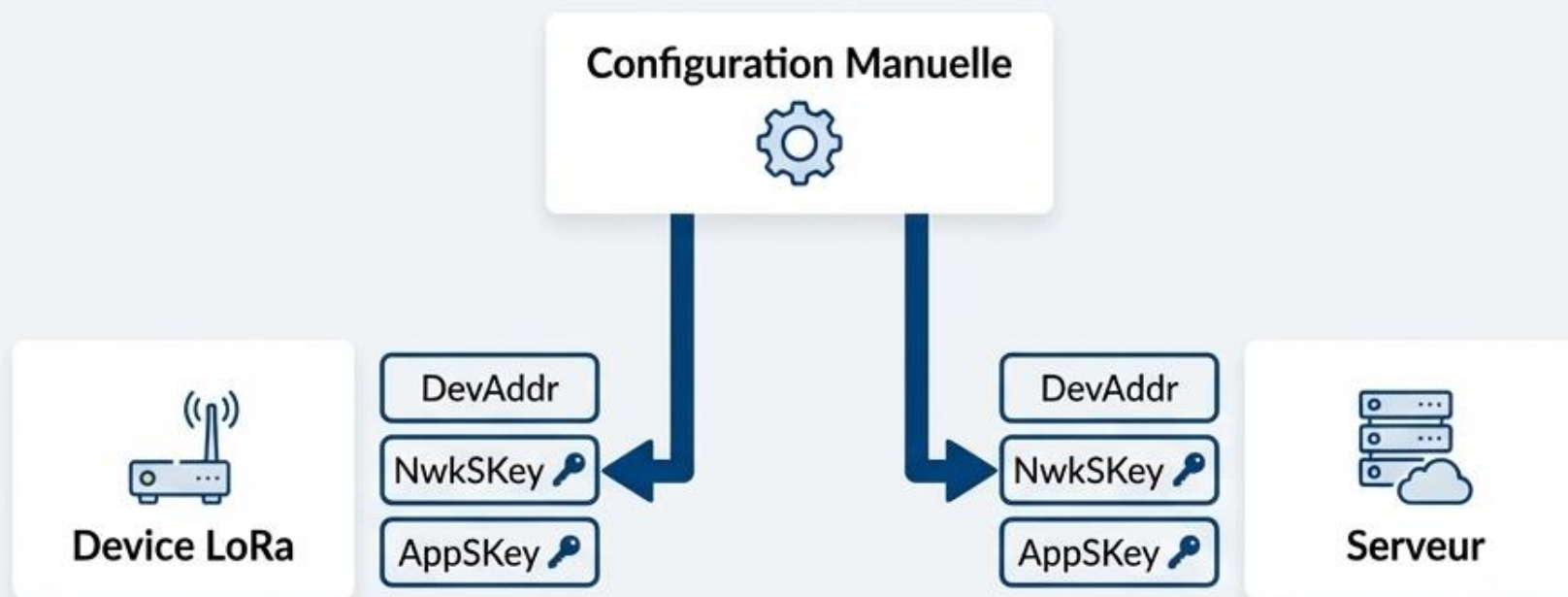


Over-The-Air Activation (OTAA)

Les clés sont négociées dynamiquement avec le réseau.

Méthode 1 : Activation By Personalization (ABP)

La méthode statique.



Avec ABP, toutes les informations (DevAddr, NwkSKey, AppSKey) sont définies et stockées en dur à la fois dans le Device LoRa et sur le serveur.

Le device peut commencer à communiquer immédiatement sans procédure d'enregistrement préalable.

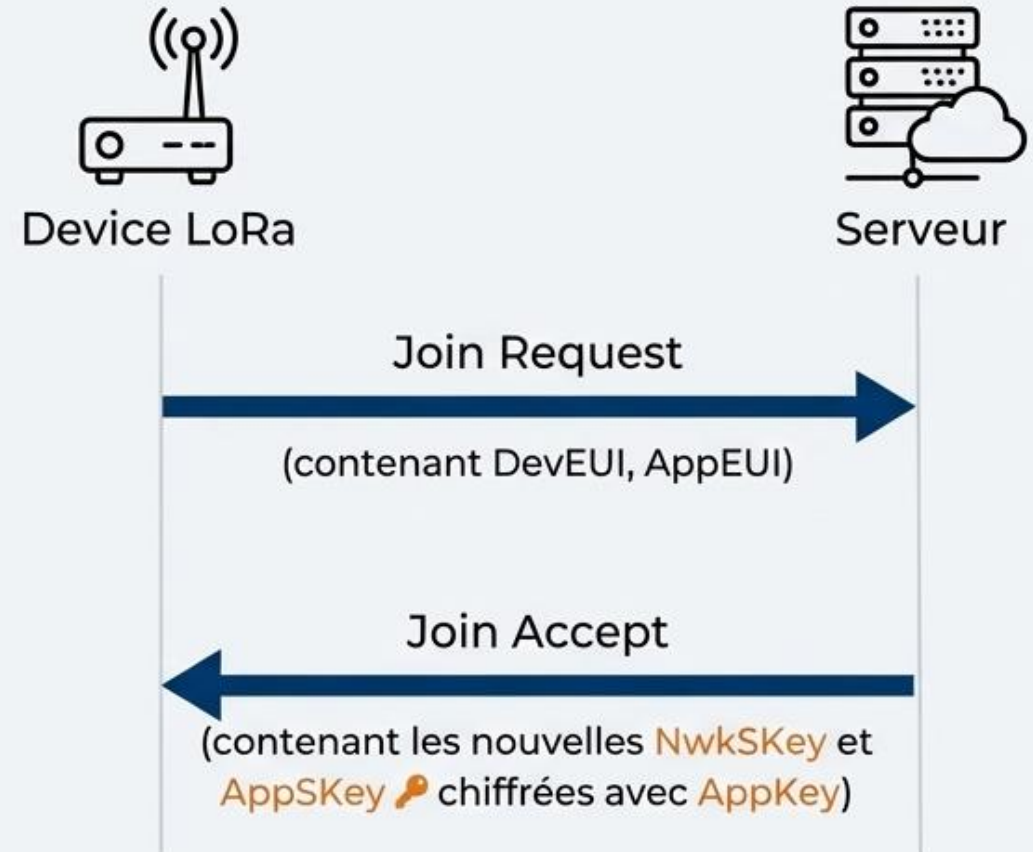
- **Avantage** : Simple et rapide pour le déploiement. ✓
- **Inconvénient** : Moins sécurisé car les clés ne changent jamais. ⚠

Méthode 2 : Over-The-Air Activation (OTAA)

La méthode dynamique et sécurisée.

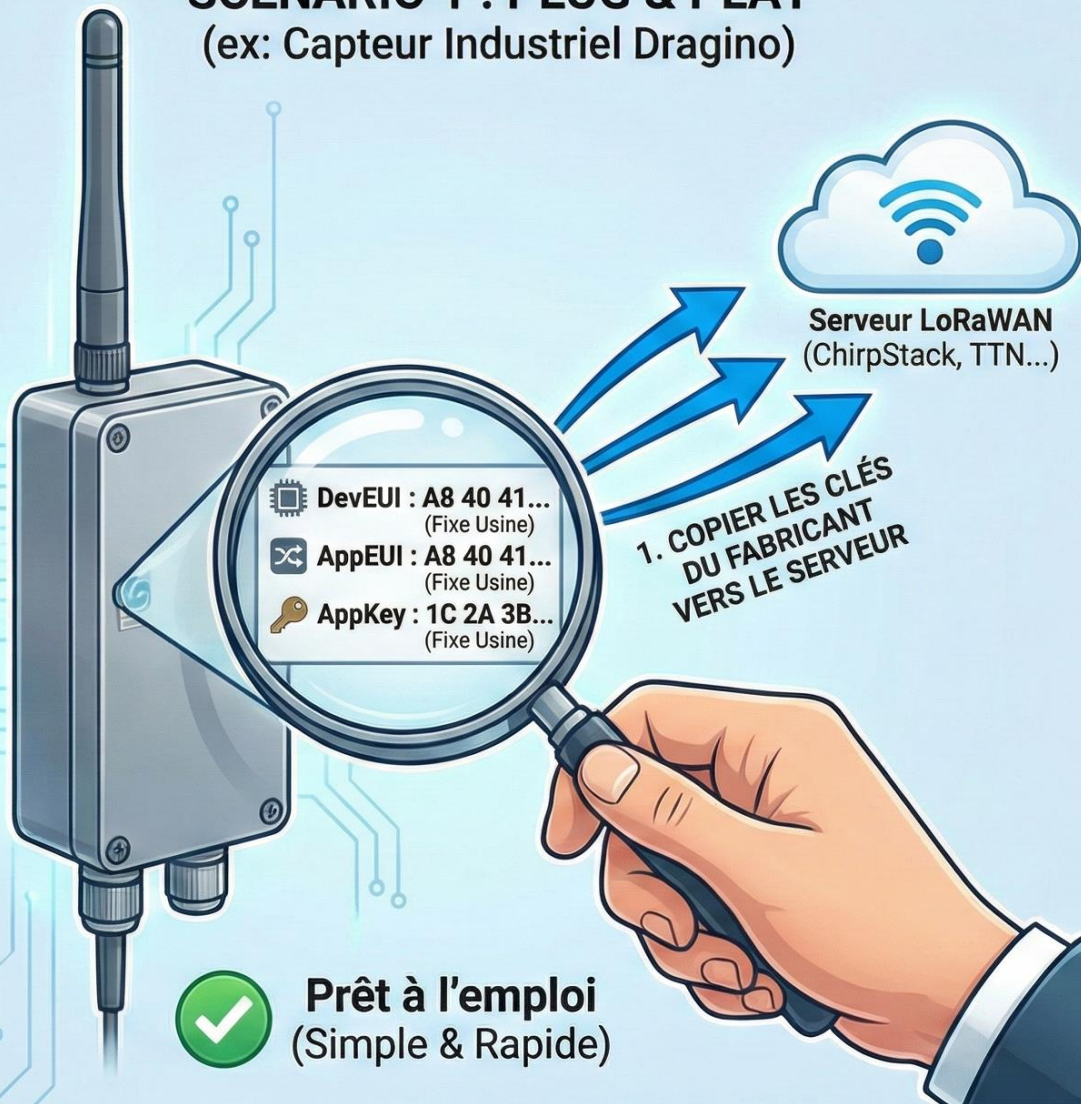
Le device possède des identifiants uniques et une clé racine (DevEUI, AppEUI/JoinEUI, AppKey). Il initie une procédure de "Join" pour s'enregistrer sur le réseau. Le serveur vérifie ses identifiants et génère dynamiquement des clés de session uniques (NwkSKey, AppSKey) pour la communication à venir.

- Avantage : Très sécurisé. Les clés de session peuvent être renouvelées. ✓

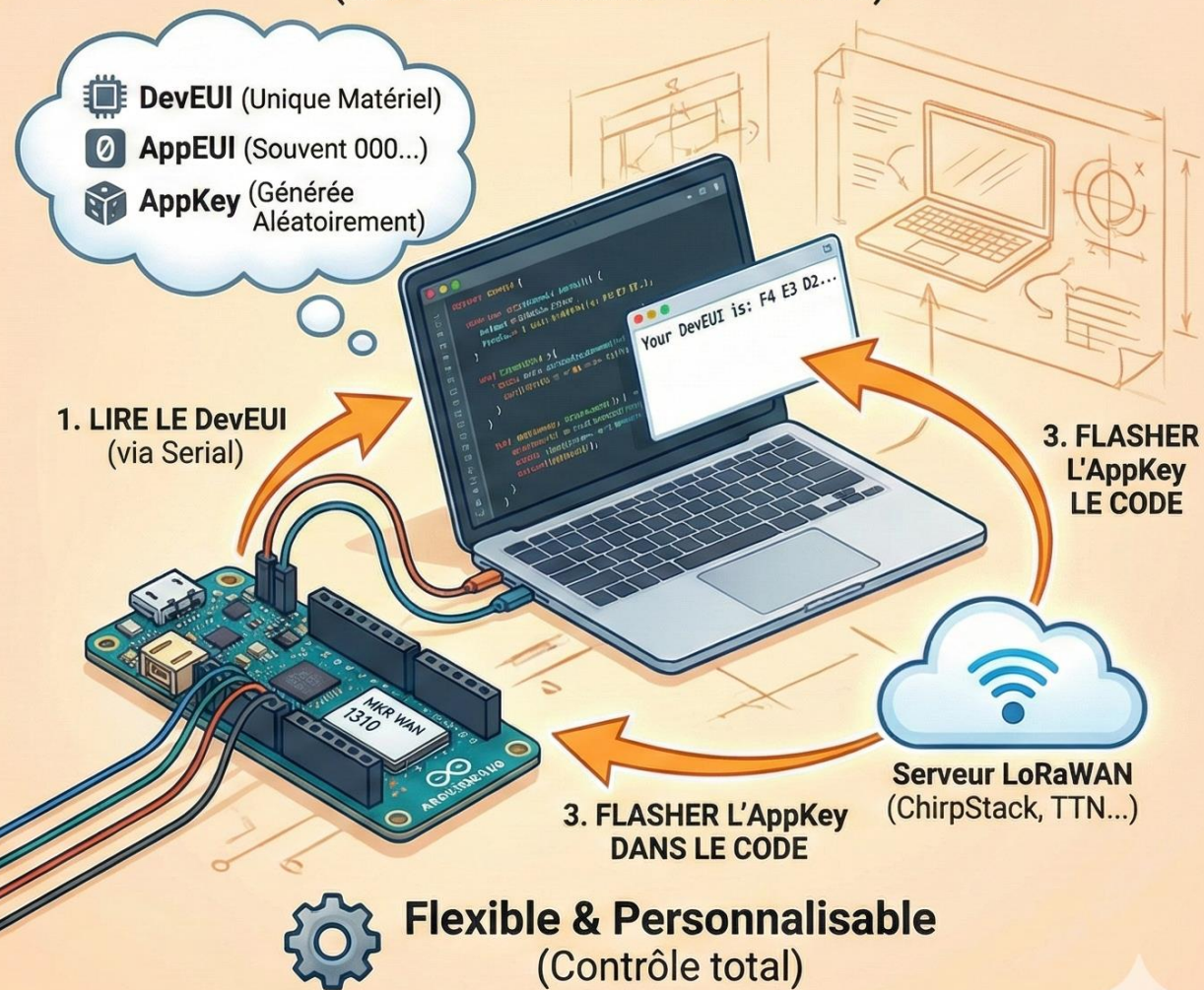


Gestion des Clés LoRaWAN : Deux Approches (OTAA)

SCÉNARIO 1 : PLUG & PLAY (ex: Capteur Industriel Dragino)




SCÉNARIO 2 : DÉVELOPPEUR (ex: Carte Arduino MKR WAN)





LÉGENDE : DevEUI (Qui suis-je ?) | AppEUI/JoinEUI (Où vais-je ?) | AppKey (Mot de passe secret)

1. L'OBJET PHYSIQUE : Capteur Dragino & Étiquette



**DevEUI : A8 40 41 C0 01 02 03 04**
(Identifiant Unique)

**AppEUI : A8 40 41 00 00 00 00 01**
(Identifiant Application)

**AppKey : 1C 2A 3B 4D 5E 6F 70
81 92 A3 B4 C5 D6 E7 F8 09**
(Clé Secrète)

Copier exactement
(Format MSB)

⚠
ATTENTION :
SECRET !

2. L'INTERFACE SERVEUR : ChirpStack (Web)

A screenshot of the ChirpStack web interface. The page title is 'ChirpStack' and the breadcrumb is 'Tableau de bord ChirpStack > Applications > Mon App > Créer un Device'. The form contains three input fields: 'Device EUI (DevEUI)' with the value 'A84041C001020304', 'Join EUI (ou AppEUI)' with the value 'A840410000000001', and 'Application Key (AppKey)' with the value '1C2A3B...*****'. A green button at the bottom says 'ENREGISTRER / CRÉER DEVICE'. A cloud icon at the bottom right is labeled 'Réseau LoRaWAN (Prêt)'.

1. RÉCUPÉRATION DU DevEUI (Arduino)

2. GÉNÉRATION DES CLÉS (ChirpStack)

3. CONFIGURATION DU SKETCH (Arduino IDE)

Copier le
DevEUI

Copier
l'AppKey
générée

Téléverser le code
& Rejoindre (OTAA)

A screenshot of the ChirpStack web interface. The title is "Créer un Device (OTAA)". There are three input fields: "Device EUI (DevEUI)" with the value "A8610A34B2C1D3E4", "Join EUI (AppEUI)" with the value "0000000000000000", and "Application Key (AppKey)" with the value "F4 E3 D2 C1 B5 A4 93 82 71 60 5F". A button labeled "Generate random key" is next to the AppKey field.A screenshot of the Arduino IDE showing a sketch for an Arduino MKR 1310. The code includes headers for LoRa and the Arduino IDE. The main function contains a configuration for the LoRa module, including the DevEUI and AppKey. The AppKey is highlighted in red in the original image.

```
Arduino_MKR_1310
#include <clatoe.h>
#include <clatoe.h>
#include <peestebwat>
#include <peestet.h>

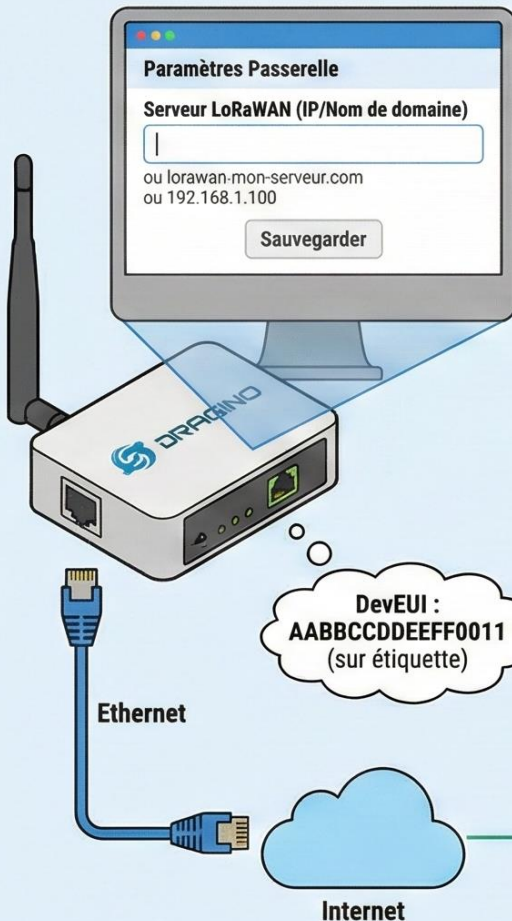
void main() {
{
// Iqert LoRa configuration
String appEui = "0000000000000000";
String appEui = under=appEui;
String appKey = "F4E3D2C1B5A4938271605F4E3D2C1B0A";

if (celio-apper=appKey) {
appEui.leack();
}

void sketch() {
```


Processus de Configuration LoRaWAN : De la Passerelle à l'Appareil (OTAA)

Étape 1 : Configuration de la Passerelle



Étape 2 : Enregistrement sur le Serveur

LoRaWAN Server (ChirpStack, TTN)

LoRaWAN

Dashboard

Passerelles

Créer Passerelle

Enregistrer une Nouvelle Passerelle

Passerelle EUI

AABBCDDDEEFF0011

Nom (optional)

Description (optional)

Créer Passerelle

Étape 3 : Création de l'Application

LoRaWAN Server

LoRaWAN

Dashboard

Applications

Créer une Nouvelle Application

Nom de l'Application

Capteurs Météo

Description

Créer Application

Capteurs Météo

Étape 4 : Ajout d'un Appareil (OTAA)

Capteurs Météo

LoRaWAN

Dashboard

Applications

Capteurs Météo

Créer un Device

Ajouter un Appareil

Méthode d'Activation

☒ OTAA (Over-the-Air Activation)

Device EUI (DevEUI)

0102030405060708

Join EUI (AppEUI)

0000000000000000

Application Key (AppKey)

Générer 1234...ABCD

Enregistrer Device