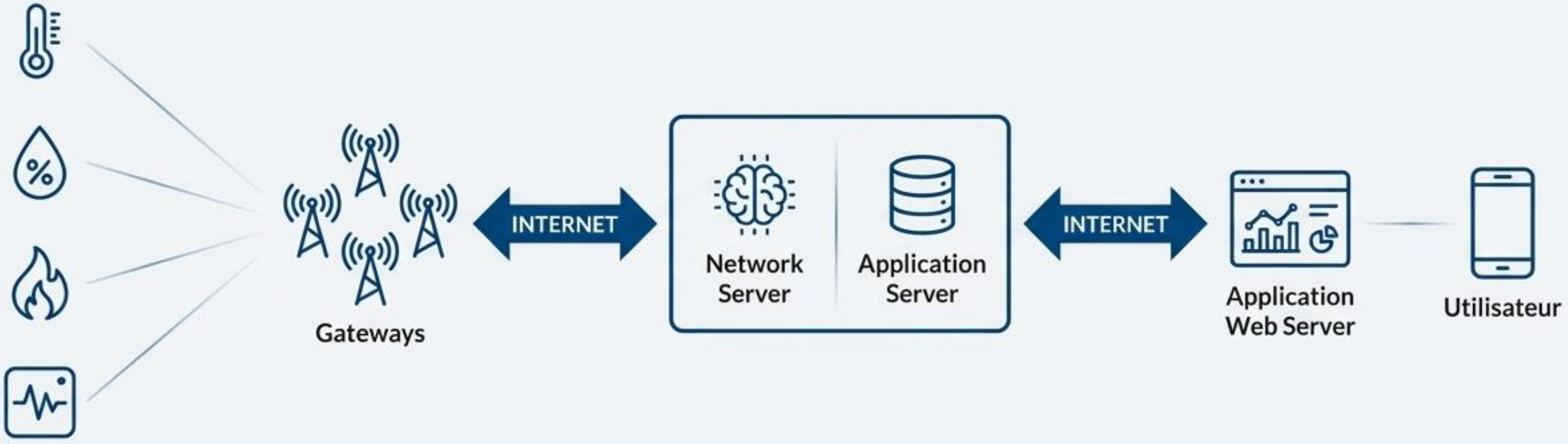
Le Voyage d'une Donnée à travers l'Architecture LoRaWAN

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

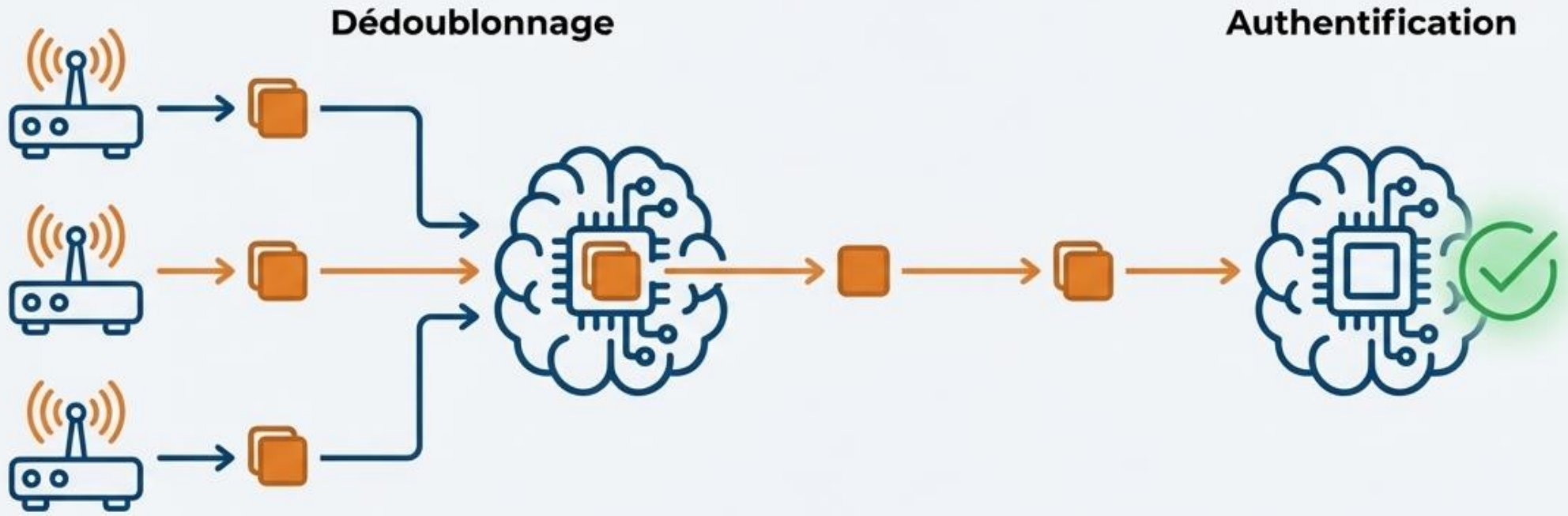
Ils **n'adressent pas une gateway spécifique.** Toutes les gateways à portée reçoivent le message, assurant la redondance et la robustesse du réseau.

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 : Dédoublonnage

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)

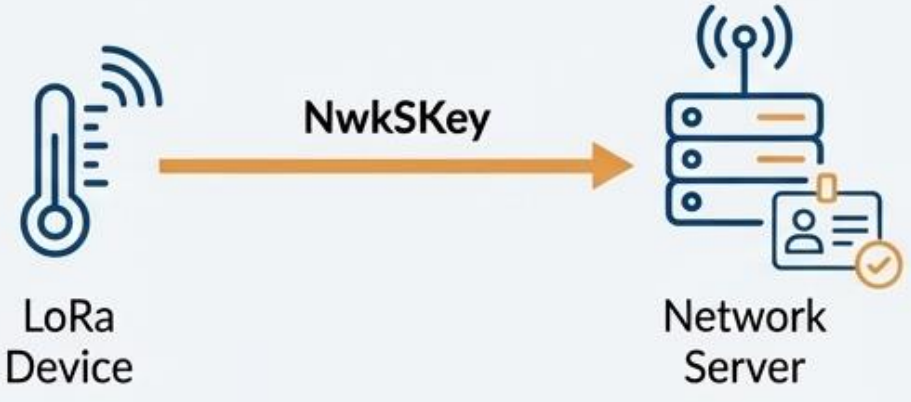
Il est également possible d’envoyer des commandes depuis l’application vers les Devices LoRa.

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.

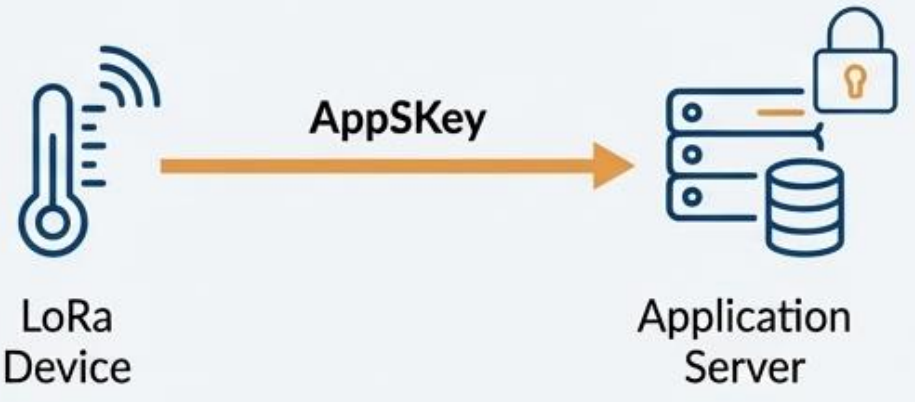
Network Session Key (NwkSKey)

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

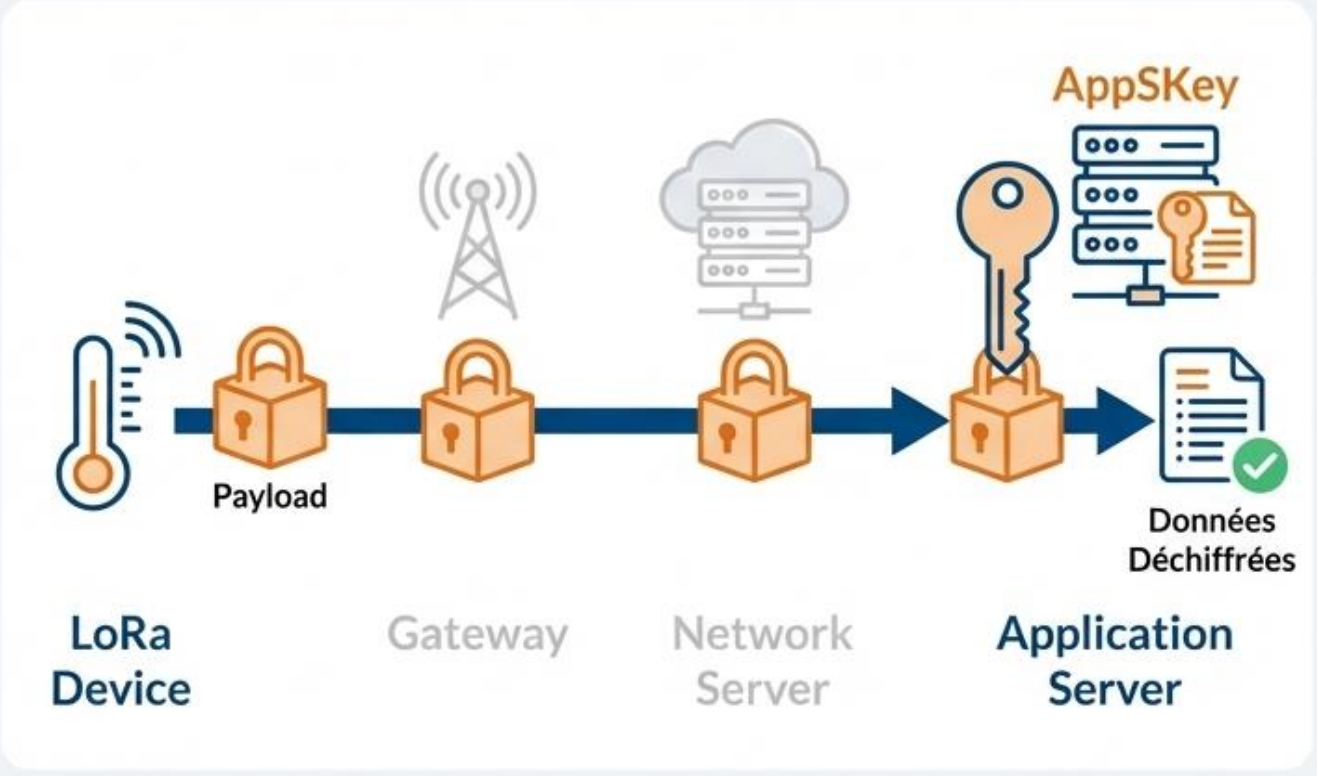
La **Network Session Key (NwkSKey)** est partagée uniquement entre le Device LoRa et le Network Server.

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.

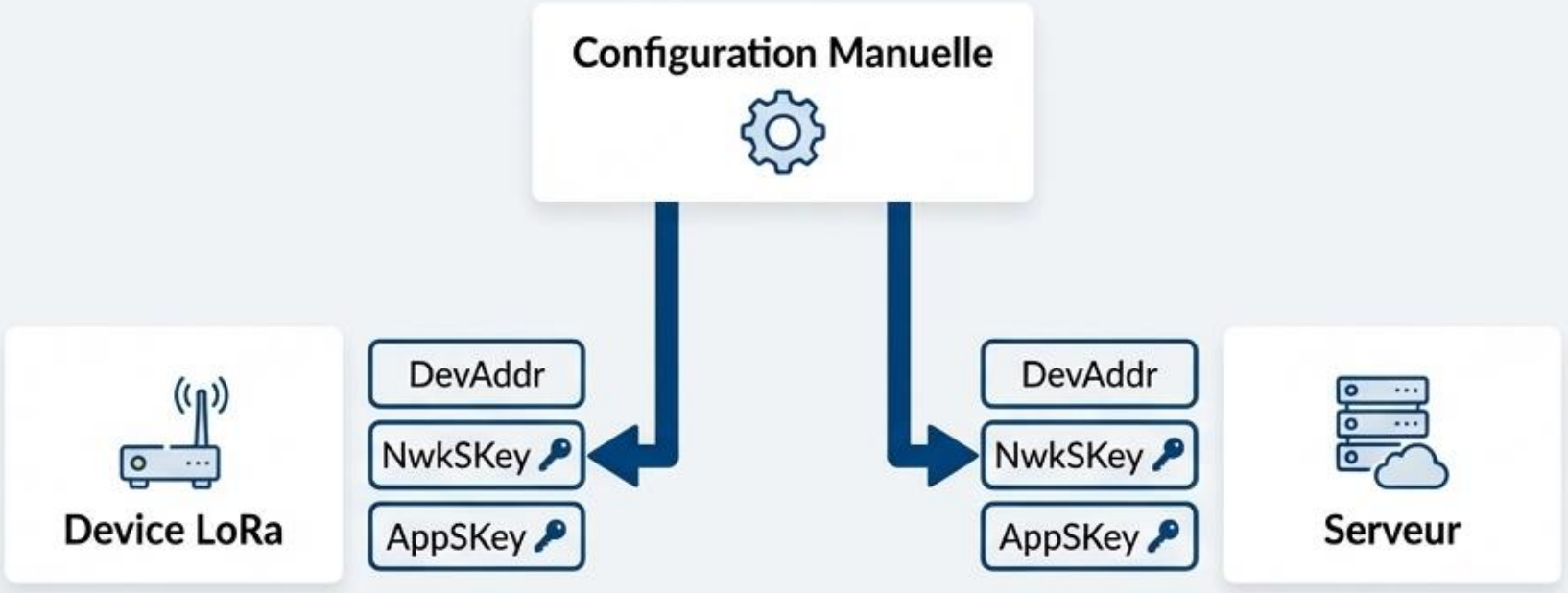
Il existe deux méthodes pour fournir ces informations au Device et au Serveur.

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. ✅