escrypt
SECURITY. TRUST. SUCCESS.

Secure LPWAN Communications

Life cycle key management for LoRaWAN networks

Secure LPWAN Communications

Low-Power Wide Area Networks (LPWAN) is a rapidly evolving technology that allows for low-cost connectivity for IoT devices and Smart City applications. LoRaWAN is a specific open standard LPWAN, driven by the LoRa Alliance, that provides independency from telecommunication providers giving users the possibility to extend their network individually to meet their needs while also remaining in charge of costs and availability. In addition, LoRaWAN has been designed from the beginning to provide strong end-to-end security model for IoT devices and network authorization.

One of the biggest challenges faced by LoRaWAN service providers is the secure provisioning and storage of device keys and activation of devices in a scalable way on their network. ESCRYPT's KMS for LoRaWAN provides a complete, turn-key, security solution for LoRaWAN deployments based on security best practices. It provides a secure key store and key derivation for network access and application servers.

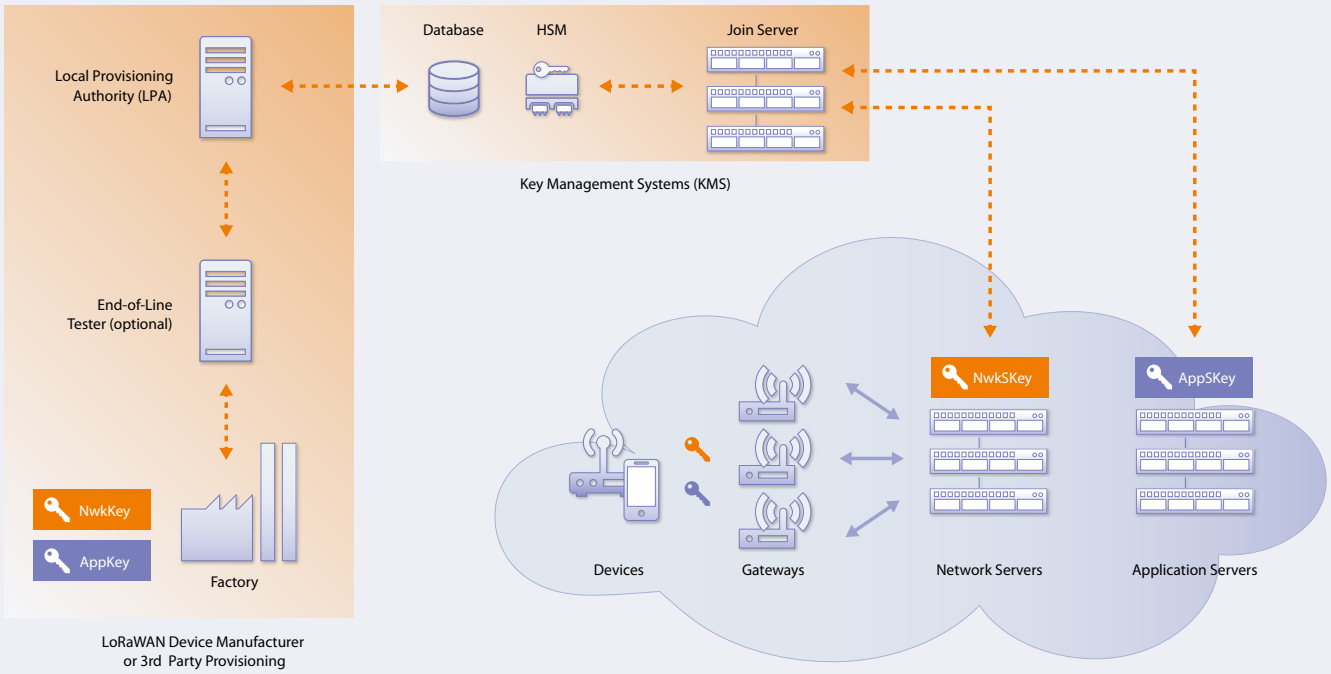
As a fully managed service, ESCRYPT's KMS/Join Server for LoRaWAN simplifies device key provisioning, storage and management by manufacturers and service providers. It also securely delivers device keys to clients and product manufacturers while offering service providers unlimited network scalability and guaranteeing that only registered devices are activated on their networks.

Unique keys are injected into new devices so that they can authenticate themselves to the LoRaWAN network and to protect the secrecy and integrity of individual applications which may operate over the same wireless infrastructure. In addition, service providers never have access to end user encryption keys further protecting the user's valuable data.

ESCRYPT 2018/05

escrypt
SECURITY. TRUST. SUCCESS.

Secure LPWAN Communications



Features

- Security Best Practices
  - Secure key generation utilizing a security protocol between Secure Element and Key Management Service (KMS) Join Server
  - Device keys and cryptography are housed in a secure execution environment
- Fully Managed Service
  - 24 x 7 x 365 availability, physical security & maintenance
  - All keying material is protected in FIPS 140-2 Level 3 Hardware Security Modules (HSMs)
- Centralized Key Management
  - Centralized control of all LoRaWAN AES device keys
  - Key generation, secure key storage & usage
  - Audit Trail
- Server Provider API & Registry
  - Secure links to registered LoRa service providers
  - Service provider independent allowing valid devices to roam
  - Automatic LoRa device registration
- Client & Manufacturing Provisioning API for LoRa Devices
  - Device manufacturers or the application owner initiated
  - Over-The-Air Activation (OTAA)
  - Can be offered through a service provider

Benefits

Secure: LoRaWAN device keys are never exposed and are reliably shared on your network with authorized clients or manufacturers; service providers never have access to end user encryption keys.

End-to-End Data Protection: Data is encrypted from device to target application server and independent of the LoRaWAN Network Service Provider.

Robust: Network security posture is improved using a proven life cycle key management solution to securely generate, provision, manage and store all LoRaWAN device keys.

Brand Protection: Secure provisioning of all LoRaWAN devices guarantees only authorized devices are activated on your network.

Ease of Integration: Easily integrate into the manufacturing process using a cloud based key management service and turn-key production ready appliances to personalize and activate any LoRaWAN device onto any network.