micromax technology

gemalto
security to be free

Gemalto Trusted Key Manager

The end-to-end security solution for IoT devices using LoRaWAN™

The Key to Trust in the LoRa® Connected Internet of Things

The Internet of Things (IoT) is transforming our world with enhanced convenience, efficiency and safety to improve the way we work and live. The pace of change is swift, but one thing is certain, for IoT to reach its full potential, people need to have confidence that IoT connected devices, data and networks are secure.

The Gemalto Trusted Key Manager gives device makers, network operators and service providers a fully-featured solution that brings end-to-end security to IoT devices connecting on the booming LoRa® networks.

Expanding LoRa Low-Power Wide-Area Networks

IHS estimates that more than 30 billion things will be connected to the Internet by 2020, and the majority of these do not require the bandwidth and speed of traditional cellular wireless networks. Instead, many devices demand cost-efficient, low-power connectivity solutions that can support long-lived global deployments.

To meet these needs, Low-Power Wide-Area Network (LPWAN) technologies have flourished, such as LoRaWAN™ (LoRa), Sigfox and NB-IoT. LoRa is the most mature and widely available of these options.

	SIGFOX	LoRa	Clean slate	NB LTE-M Rel. 13	LTE-M Rel. 13	EC-GSM Rel. 13	5G (targets)
Range (outdoor) MCL	< 13km 160 dB	< 11km 157 dB	< 15km 164 dB	< 15km 164 dB	< 11km 156 dB	< 15km 164 dB	< 15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10kbps	<50kbps	<150kbps	<1Mbps	<10kbps	<1Mbps
Battery life	> 10 years	> 10 years	> 10 years	> 10 years	> 10 years	> 10 years	> 10 years

Source: Lemag numerique – Oct 2016

LoRaWAN was specifically designed to deliver wireless connectivity for battery-powered things that need to operate for a decade or more. It offers extreme efficiency and provides long-range connectivity making it ideal for cost sensitive applications deployed in hard-to-reach locations.

Because security and trust are paramount to the success of the LoRa technology, the LoRa Alliance™ specified strong security architecture requirements. As an active LoRa Alliance sponsor, Gemalto developed the Trusted Key Manager to secure the LoRa ecosystem and lifecycle and meet all Alliance requirements.

The Solution Architecture

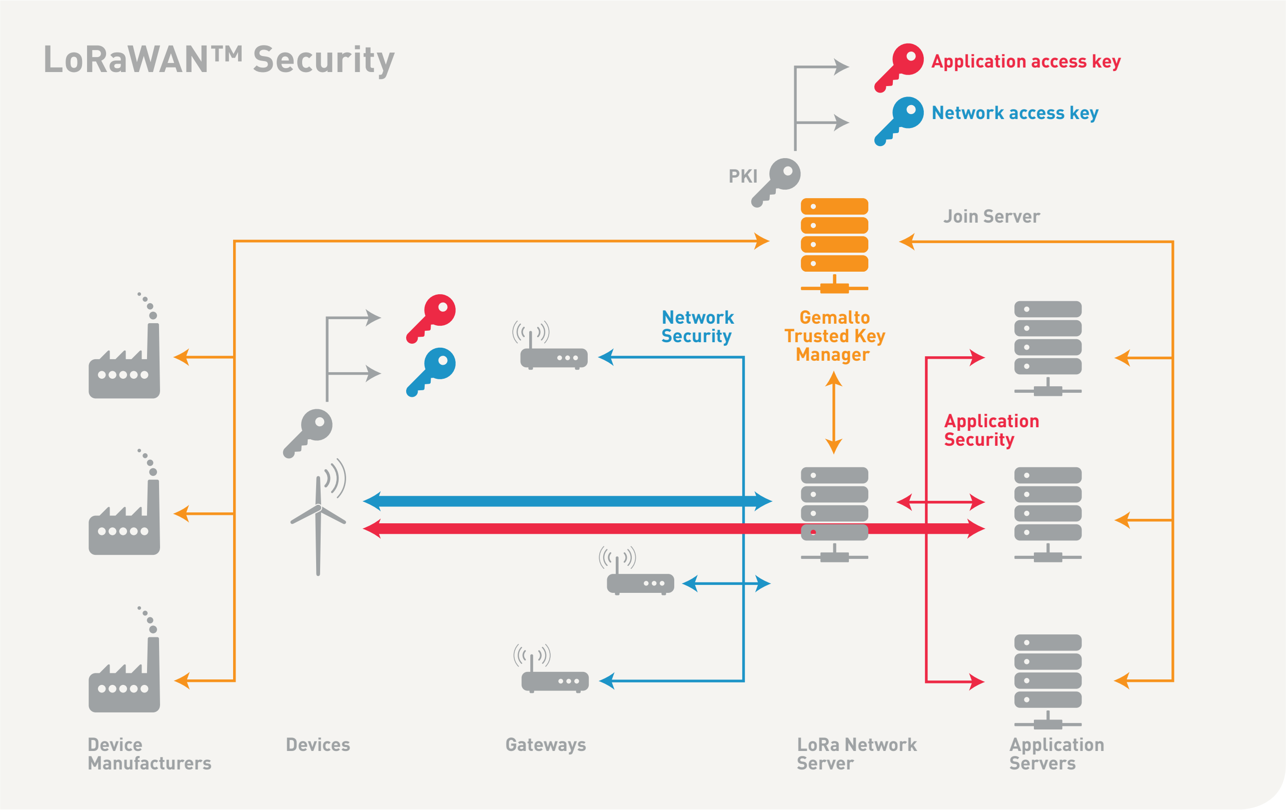
The Gemalto Trusted Key Manager (TKM) solution safeguards the integrity of LoRa networks, devices and data by providing 3 levels of remote credential provisioning for:

1. LoRa devices
2. LoRa networks
3. Application servers that need access to device data

Unlike traditional cellular IoT devices, LoRa-based devices do not use SIM cards for authentication. Instead, LoRa-based devices are generic and can be operated on any LoRa network. The network routes a device ´join request´ to its ´join server´ - the back-end entity that manages the device activation. Gemalto TKM, a LoRa join server, thus facilitates a strong mutual authentication process between the IoT device and the LoRa network, to ensure the integrity of LoRa IoT solutions.

The secure handshake between the device and the network leverages market proven, standardized AES cryptographic algorithms for key credential generation. This delivers a highly-reliable join procedure. The remote, double key provisioning mechanism ensures that only authorized devices can connect to authorized networks.

In addition to authentication between the device and network, another set of keys is provisioned at application level for mutual authentication between the device and the application servers. This ensures complete data confidentiality for application servers or solution providers who are given specific keys to access the device data they are authorized to see. Leveraging recognized encryption techniques, the Gemalto Trusted Key Manager also ensures that data transferred over the network has not been altered, is coming from a legitimate source and is undecipherable to eavesdroppers.



Just like LoRaWAN, the Gemalto Trusted Key Manager supports low implementation complexity, cost economy and high scalability, leaving the complete management of credential provisioning and deployment to an external security expert entity. The solution is available as a cloud or as a dedicated in-house platform installed on customer premises.

IoT Ecosystem Benefits

Leveraging decades of experience successfully managing secure provisioning and authentication in the banking and telecommunications sectors, the Gemalto Trusted Key Manager benefits all LoRaWAN ecosystem players:

IoT Device Makers

- Removes the burden of security provisioning, saving time and money
- Generic devices allow IoT device onboarding on any LoRaWAN network
- Simplifies device lifecycle management with automated and secure network ´join process´

LoRa Network Operators

- Simplifies device network onboarding and allows seamless LoRa network operator change, which is crucial when, for instance, devices change ownership

IoT Application Servers and End Users

- Ensures complete confidentiality and integrity of accessed data

The Gemalto Trusted Key Manager strengthens the LoRa security ecosystem and allows all the stakeholders to trust the integrity of both devices and data. The solution gives businesses and people the confidence they need to embrace our connected world and unleash the power of the IoT.

For more information, visit our dedicated webpage.

LoRa, LoRaWAN and the LoRa Alliance are marks used under license from the LoRa Alliance.