FREQUENTLY ASKED QUESTIONS

01. Where are the LoRaWAN™ security mechanisms specified?

All security mechanisms are specified in the LoRa Alliance™ specifications that can be downloaded by the public from https://www.lora-alliance.org/Contact/RequestSpecificationForm.aspx

Currently, LoRaWAN Release 1.0 and 1.0.2 are available for download. Release 1.1 is under construction. This FAQ is based on the LoRaWAN 1.0.x specifications.

02. How do the LoRa Alliance specifications ensure secure operation of LoRaWAN networks?

LoRaWAN supports origin authentication, integrity and replay protection of the complete Media Access Control (MAC) frame. It also enables end-to-end encryption of the application payload between the end-device and its counter-part on the network side (which is called the Application Server in Release 1.1). LoRaWAN supports a mode of operation that allows encryption of the MAC commands.

All of these procedures rely on the Advanced Encryption Standard (AES) and use 128-bit cryptographic keys and algorithms.

03. Are there any differences between the ABP (Activation-by-Personalization) and OTAA (Over-the-Air-Activation) methods in terms of security?

LoRaWAN uses static root keys and dynamically-generated session keys.

Root keys are only provisioned in OTAA end-devices. They are used to derive session keys when the OTAA end-device executes a Join Procedure with the network. An OTAA end-device, when installed in the field, will be able to connect to any network that has an interface to the key server (which is called a Join Server in Release 1.1) to which the end-device is associated. Session keys are used by the end-devices to protect the over-the-air traffic.

ABP end-devices are not provisioned with the root keys. Instead, they are provisioned with a set of session keys for a pre-selected network. The session keys remain the same throughout the lifetime of an ABP end-device.

The ability to rekey session keys makes OTAA devices more suitable for applications requiring a higher level of security.

04. What kind of identifiers are used in LoRaWAN?

Each end-device is identified by a 64-bit globally unique Extended Unique Identifier (EUI-64) that is assigned either by the manufacturer or the owner of the end-device. Allocation of EUI-64 identifiers require the assignor to have an Organizationally Unique Identifier (OUI) from the IEEE Registration Authority.

Each Join Server, which is used for authenticating the end-devices, is also identified by a 64-bit globally unique identifier (EUI-64) that is assigned by either the owner or the operator of that server.

Open LoRaWAN networks and private LoRaWAN networks that are collaborating (roaming) with the open networks are identified by a 24-bit globally unique identifier assigned by the LoRa Alliance.

When an end-device successfully joins a network, it gets a 32-bit ephemeral device address assigned by the serving network.

05. Can I randomly assign any identifier to my device or my network?

No. Please see question #4 about the assignment authority for each identifier. Not following these guidelines would cause identifier collision and unpredictable behavior in your network deployment (similar to what happens when using the same Ethernet MAC address on multiple devices attached to the same LAN).

06. Are all end-devices equipped with the same "default" cryptographic key when leaving the manufacturer?

No. There is no concept of a "default key" or a "default password" in LoRaWAN. All end-devices are equipped with unique keys when they leave the manufacturer. As a consequence, any compromise of a key from one end-device will not have an impact on other end-devices.

FREQUENTLY ASKED QUESTIONS

07. What kind of cryptographic keys are used?

An OTAA end-device is provisioned with a root key called the Application Root Key (AppKey). On the network side, AppKey is provisioned on the Join Server, which may or may not be co-located with the Network Server.

An ABP end-device is provisioned with two session keys (called the Application Session Key, AppSKey and the Network Session Key, NwkSKey). On the network side, the NwkSkey is provisioned on the Network Server and the AppSKey is provisioned on the Application Server.

The procedures used for provisioning the aforementioned keys on the required elements (end-device, Join Server, Network Server, Application Server) are outside the scope of the LoRaWAN specification.

08. What kind of cryptographic algorithms are used?

The AES-CMAC mode of operation as defined in RFC4493 is used for origin authentication and integrity protection. AES-CCM* mode of operation as defined in IEEE 802.15.4-2011 is used for encryption.

09. How does LoRaWAN prevent eavesdropping?

The MAC payload is encrypted between the end-device and the network as it is transmitted over the air. Additionally, the application payload is encrypted between the end-device and the Application Server (i.e., end-to-end). This ensures only the authorized entities that hold the decryption keys can access the plain-text content.

10. How does LoRaWAN prevent spoofing?

The MAC payload is origin authenticated and integrity protected with the help of a Message Integrity Code (MIC) field between the end-device and the network. This ensures only the authorized entities that hold the integrity keys (i.e., the end-device and the Network Server) can generate valid frames.

11. How does LoRaWAN prevent replay attacks?

Integrity protection of the MAC payload utilizes frame counters to ensure the receiver does not accept an already received (i.e., potentially replayed) frame.

12. Does LoRaWAN support security for application payloads?

LoRaWAN enables end-to-end encryption of the application payload between the end-device and the Application Server. Integrity protection is provided in a hop-by-hop nature: one hop over the air through the integrity protection provided by LoRaWAN and the other hop between the Network Server and the Application Server by using secure transport solutions such as HTTPS and VPNs. Applications in need of end-to-end integrity protection are encouraged to do so within their application payloads.

13. How are the backend interfaces secured?

The backend interfaces involve control and data signaling among Network Servers, Join Servers and Application Servers. HTTPS and VPN technologies are recommended for securing the communication among these critical infrastructure elements, in much the same way as is done in any other telecom systems. Backend interfaces is outside the scope of LoRaWAN specification.

14. Does LoRaWAN support hardware security?

Enhanced security of the end-devices and server platforms by means of using hardware security (e.g., Secure Elements or Hardware Security Modules) are implementation matters and not related to protocol interoperability aimed by telecommunication specifications, including LoRaWAN. Nevertheless, use of such techniques are compatible with the LoRaWAN specifications and should be implemented by the developer as required by the application.

15. What should I do if I identify a security threat?

Generally speaking, a given security threat may arise from the specification (e.g., lack of replay protection), the implementation (e.g., key extraction on the device), the deployment (e.g., lack of firewalls) or a combination of these three.

The LoRa Alliance works towards ensuring its specifications are secure while recognizing the overall security of the solution also depends on the implementation and deployment security. In the face of a security threat the first action is to identify the source of the threat. If it is related to the LoRaWAN specification, the LoRa Alliance is the right place to address it (help@lora-alliance.org).

On the other hand, implementation security issues need to be taken up by the relevant manufacturers and deployment issues need to be taken up with the relevant network operator(s). These two types of threats are not specific to the LoRaWAN technology and are usually equally applicable to any radio technology which may be implemented on the same platforms/networks.

LoRa Alliance™
Wide Area Networks for IoT

LoRaWAN™ Specification, v1.0.2, July 2016
LoRa Alliance™: **www.lora-alliance.org**
media@lora-alliance.org