



LoRaWAN™ SECURITY



**FULL END-TO-END ENCRYPTION
FOR IoT APPLICATION PROVIDERS**

**A WHITE PAPER PREPARED FOR
THE LoRa ALLIANCE™**
BY GEMALTO, ACTIVITY AND SEMTECH
February 2017



INTRODUCTION

LoRaWAN™ is a Low Power Wide Area Network (LPWAN) protocol that supports low-cost, mobile, and secure bi-directional communication for Internet of Things (IoT), machine-to-machine (M2M), smart city, and industrial applications. The LoRaWAN protocol is optimized for low power consumption and is designed to support large networks with millions of devices. Innovative LoRaWAN features include support for redundant operation, geolocation, low-cost, and low-power applications. Devices can even run on energy harvesting technologies enabling the mobility and ease of use of IoT.

As security is a fundamental need in all of the aforementioned applications, it has been designed into the LoRaWAN specification from the very beginning. However, the topic of security encompasses multiple properties and, in particular, the cryptographic mechanisms used to implement security in LoRaWAN deserve careful explanation. This whitepaper aims to present the security of the current LoRaWAN specification. First, we will present the security properties embodied in the LoRaWAN specifications, then details of its implementation and finally some explanations about LoRaWAN security design.

PROPERTIES OF LoRaWAN™ SECURITY

LoRaWAN security is designed to fit the general LoRaWAN design criteria: low power consumption, low implementation complexity, low cost and high scalability. As devices are deployed in the field for long periods of time (years), security must be future-proof. The LoRaWAN security design adheres to state-of-the-art principles: use of standard, well-vetted algorithms, and end-to-end security. Later, we describe the fundamental properties that are supported in LoRaWAN security: mutual authentication, integrity protection and confidentiality.

Mutual authentication is established between a LoRaWAN end-device and

the LoRaWAN network as part of the network join procedure. This ensures that only genuine and authorized devices will be joined to genuine and authentic networks.

LoRaWAN MAC and application messaging are origin authenticated, integrity protected, replay protected, and encrypted. This protection, combined with mutual authentication, ensures that network traffic has not been altered, is coming from a legitimate device, is not comprehensible to eavesdroppers and has not been captured and replayed by rogue actors.

LoRaWAN security further implements end-to-end encryption for application

payloads exchanged between the end-devices and application servers. LoRaWAN is one of the few IoT networks implementing end-to-end encryption. In some traditional cellular networks, the traffic is encrypted over the air interface, but it is transported as plain text in the operator's core network. Consequently, end users are burdened by selecting, deploying and managing an additional security layer (generally implemented by some type of VPN or application layer encryption security such as TLS). This approach is not suited in LPWANs where over-the-top security layers add considerable additional power consumption, complexity and cost.

SECURITY IMPLEMENTATION

The security mechanisms mentioned previously rely on the well-tested and standardized AES¹ cryptographic algorithms. These algorithms have been analysed by the cryptographic community for many years, are NIST approved and widely adopted as a best security practice for constrained nodes and

networks. LoRaWAN security uses the AES cryptographic primitive combined with several modes of operation: CMAC² for integrity protection and CTR³ for encryption. Each LoRaWAN device is personalized with a unique 128 bit AES key (called AppKey) and a globally unique identifier (EUI-64-based DevEUI), both of

which are used during the device authentication process. Allocation of EUI-64 identifiers require the assignor to have an Organizationally Unique Identifier (OUI) from the IEEE Registration Authority. Similarly, LoRaWAN networks are identified by a 24-bit globally unique identifier assigned by the LoRa Alliance™.

SECURING APPLICATION PAYLOADS

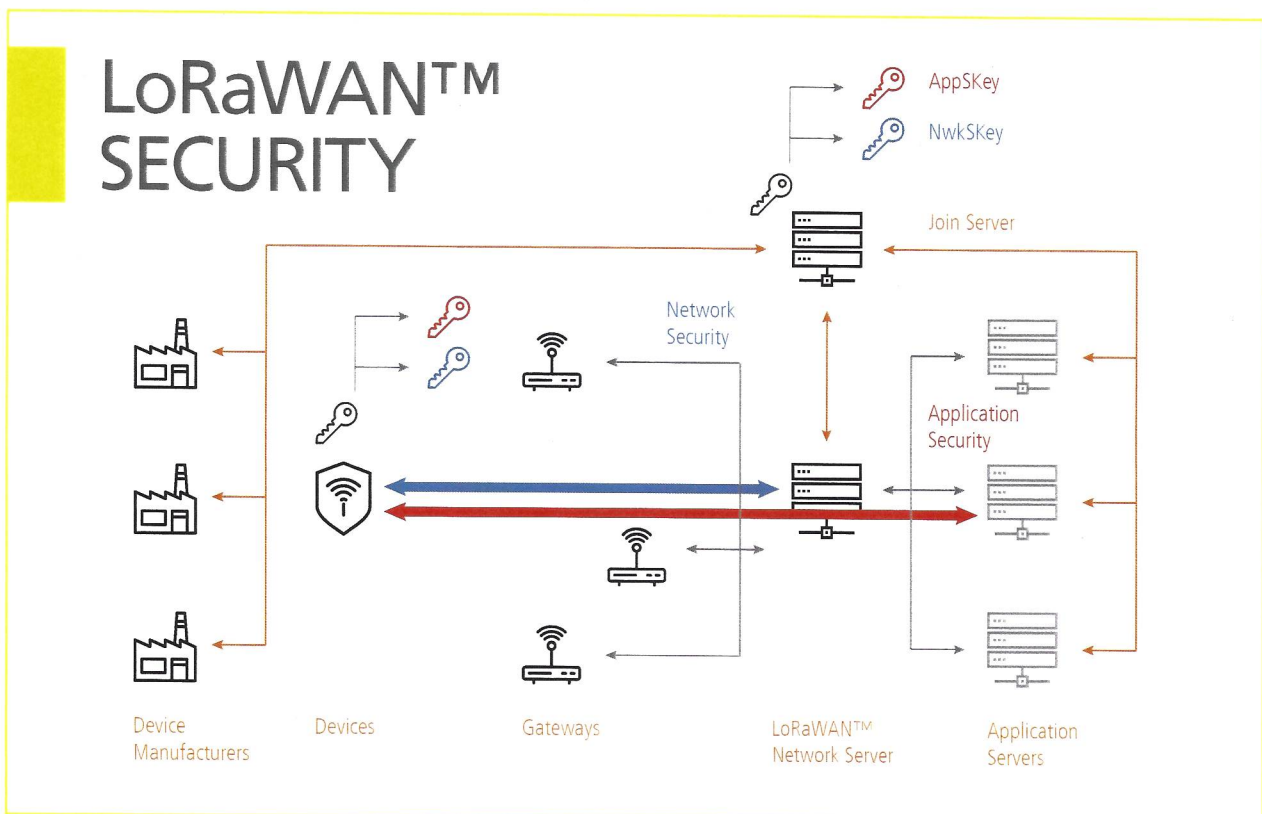
LoRaWAN™ application payloads are always encrypted end-to-end between the end-device and the application server. Integrity protection is provided in a hop-by-hop nature: one hop over the air through the integrity protection provided by LoRaWAN protocol and the other hop between the network and application server by using secure transport solutions such as HTTPS and VPNs.

MUTUAL AUTHENTICATION

The Over-the-Air Activation (a.k.a. Join Procedure) proves that both the end device and the network have the knowledge of the AppKey. This proof is made by computing an AES-CMAC⁴ (using the AppKey) on the device's join request and by the backend receiver. Two session keys

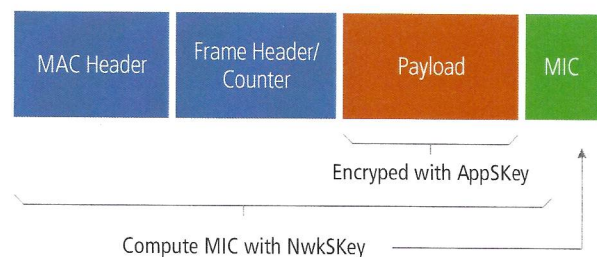
are then derived, one for providing integrity protection and encryption of the LoRaWAN MAC commands and application payload (the NwkSKey), and one for end-to-end encryption of application payload (the AppSKey). The NwkSKey is distributed to the LoRaWAN network in

order to prove/verify the packets authenticity and integrity. The AppSKey is distributed to the application server in order to encrypt/decrypt the application payload. AppKey and AppSKey can be hidden from the network operator so that it is not able to decrypt the application payloads.



DATA INTEGRITY AND CONFIDENTIALITY PROTECTION

All LoRaWAN traffic is protected using the two session keys. Each payload is encrypted by AES-CTR and carries a frame counter (to avoid packet replay) and a Message Integrity Code (MIC) computed with AES-CMAC (to avoid packet tampering). See beside the structure of a LoRaWAN packet and its protection:



SECURITY FACTS AND FALLACIES

PHYSICAL SECURITY OF A LoRaWAN™ DEVICE

AppKey and the derived session keys are persistently stored on a LoRa Alliance™ device and their protection depends on the device physical security. If the device is subject to physical threats, keys can be protected in tamper resistant storage (a.k.a. Secure Element), where they will be extremely difficult to extract.

CRYPTOGRAPHY

Some sources claim that LoRaWAN™ cryptography only uses XOR and not AES. In fact, as already mentioned, AES is used in the standardised CTR mode which makes use of XOR crypto operations (as many other modes like CBC⁵). This strengthens the AES algorithm by using a unique AES key for each block cipher.

SESSION KEY DISTRIBUTION

As AppKey and NwkKey are generated from the same AppKey, one could argue that if the LoRaWAN operator has the AppKey, it is able to derive the AppKey and hence to decrypt the traffic. In order to avoid this situation, the server managing the AppKey storage, mutual

authentication and key derivation can be run by an entity outside the control of the operator. In order to give operators additional flexibility, a future release of the LoRaWAN specification (1.1) defines two independent master keys: one for the network (NwkKey) and one for the applications (AppKey).

BACKEND INTERFACES SECURITY

The backend interfaces involve control and data signaling among network and application servers. HTTPS and VPN technologies are used for securing the communication among these critical infrastructure elements, much the same way done in any other telecom systems.

IMPLEMENTATION AND DEPLOYMENT SECURITY

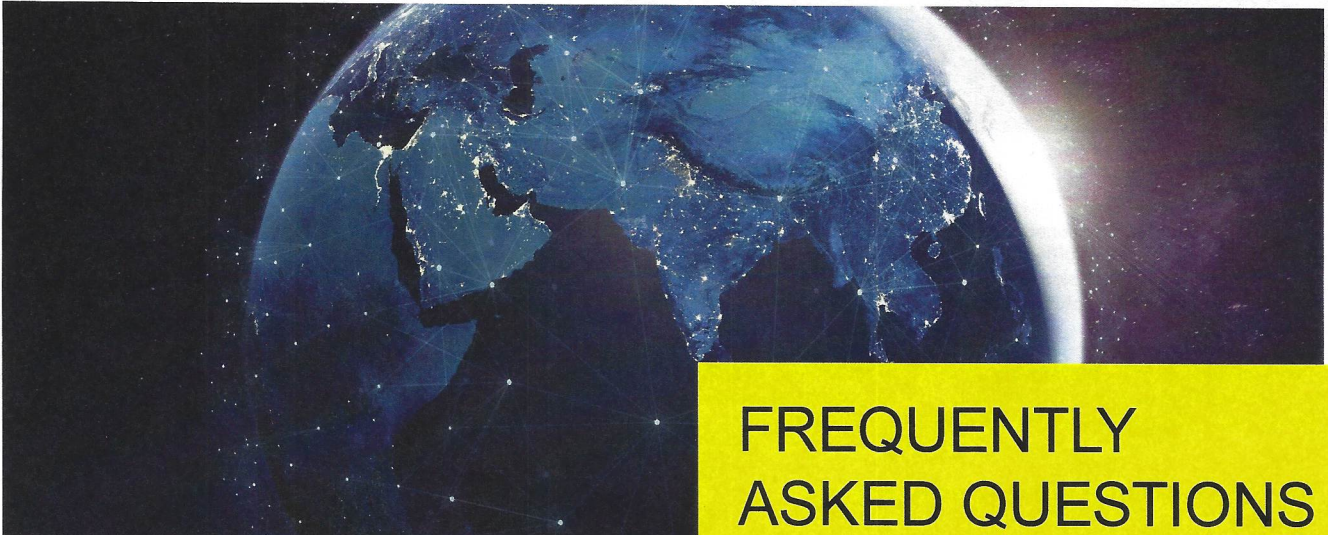
The LoRa Alliance works towards ensuring its protocol and architecture specifications are secure, while recognizing that the overall security of the solution also depends on the specific implementation and deployment. Implementation security issues need to be taken up by the relevant manufacturers and deployment issues need to be taken up by the relevant network operators. These two types of issues are not specific to the LoRaWAN technology and usually equally applicable to any radio technology implemented on the same platforms/networks.

AS SHOWN IN THIS PAPER, THE LoRaWAN™ SPECIFICATION HAS BEEN DESIGNED FROM THE ONSET WITH SECURITY AS AN ESSENTIAL ASPECT, PROVIDING STATE-OF-THE-ART SECURITY PROPERTIES FOR THE NEED OF HIGHLY-SCALABLE LOW POWER IOT NETWORKS. UNLIKE MANY OTHER IOT TECHNOLOGIES, IT ALREADY OFFERS DEDICATED END-TO-END ENCRYPTION TO APPLICATION PROVIDERS.



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

¹ AES - Advanced Encryption Standard. It is a public encryption algorithm based on symmetric secret keys, allowing message encryption and authentication. ² CMAC - Cipher-based Message Authentication Code. ³ CTR - Counter Mode Encryption. It is a mode of operation of AES algorithm relying on a counter to encrypt streams of data. ⁴ AES-CMAC - Cipher-based Message Authentication Code using AES encryption algorithm to provide message integrity and authenticity. ⁵ CBC is a mode of operation of AES algorithm relying on an initialization vector and the previous data block to encrypt streams of data.



FREQUENTLY ASKED QUESTIONS

01. Where are the LoRaWAN® security mechanisms specified?

All security mechanisms are defined in the LoRa Alliance® specifications, which can be downloaded by the public from <https://lora-alliance.org/resource-hub>. This FAQ is based on the LoRaWAN L2 1.0.3 specification.

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

LoRaWAN supports mutual end-point authentication, data origin authentication, integrity and replay protection. It also enables end-to-end encryption of the application payload between the end-device and its counter-part on the network side, the Application Server. 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 Activation by Personalization (ABP) and Over-the-Air-Activation (OTAA) 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, the Join Server, 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.

OTAA should be preferred over ABP for end-devices in need of higher levels of security.

04. What kind of identifiers are used in LoRaWAN?

Each end-device is identified by a 64-bit globally unique identifier, DevEUI, that is assigned either by the manufacturer or the owner of the end-device. Allocation of DevEUI 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, AppEUI/JoinEUI, 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, NetID, assigned by the LoRa Alliance.

When an end-device successfully joins a network, it gets a 32-bit ephemeral device address, DevAddr, 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 required to be 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.

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.

FREQUENTLY ASKED QUESTIONS

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 L2 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.

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 and 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 interoperability specification (e.g., lack of replay protection), the implementation (e.g., key extraction on the device), the deployment (e.g., lack of firewalls protecting the servers) or a combination of these three.

The LoRa Alliance ensures its interoperability 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 specifications, 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 devices/networks.



LoRaWAN® Specification, Security FAQ v2, February 2020
www.lora-alliance.org
admin@mail.lora-alliance.org

LoRa Alliance® and LoRaWAN® are registered trademarks.