sigfox

Secure Sigfox Ready™ devices

Recommendation guide

TABLE OF CONTENTS

Glossary

Below are the definitions of acronyms used in this document.

ACRONYM	DEFINITION
BS	Base Station
CTR	Counter
Device ID	Device Identifier
HSM	Hardware Security Module
MAC	Message Authentication Code
MCU	Micro Controller Unit
MK	Master Key
NAK	Network Authentication Key
ODM	Original Device Maker
OEM	Original Equipment Maker
PCI	Payment Card Industry
POS	Point Of Sale
PUF	Physical Unclonable Functions
SE	Secure Element
SEQ	Sequence Number

1 Introduction

In the Sigfox ecosystem, the design and manufacturing of Sigfox Ready devices and Sigfox Verified sub-systems is under the responsibility of third parties. These third parties could be OEMs, ODMs, Silicon vendors, module vendors or customers.

This responsibility includes design and implementation of sufficient security measures to protect customer applications, network access credentials and data conveyed on the network. Therefore, the question arises of what measures should be mandatory and whether certification or verification of the device security should be required.

This document studies the risks related to insufficient security in Sigfox Ready devices in order to raise awareness on this issue within Sigfox and throughout the Sigfox ecosystem. It is also a guide to decide what measures could be required in the design, implementation and manufacturing of Sigfox Ready devices.

2 Sigfox Ready devices security requirements

2.1 End-to-end system overview

The Sigfox network provides a cost effective and global connectivity to devices that do not need to exchange a huge amount of data with application servers. A typical case is sensors that send periodically values (temperature, GPS position…) or alarm devices that send very sporadic messages triggered by rare events.
Sigfox Ready devices send a limited number of messages per day (140 at most) with a short payload size (12 bytes max.) at a limited bitrate (in ETSI zone, 100 bits/s).

The process of this message emission is represented by the figure below.

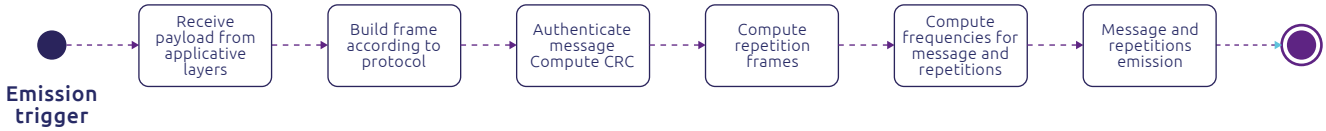

Figure 1: Device message emission process

Each message is received by one or several base stations that perform preliminary checks, then relay it to the Sigfox Core network.

When receiving a message from a base station (BS), the Core Network proceeds to verifications, which are summarized below, before delivering it to the application provider via a callback.

If the device supports it and requests it, a response can be returned. There is no way to send an unsolicited message from the server to the device, as only a device can trigger a bi-directional communication.

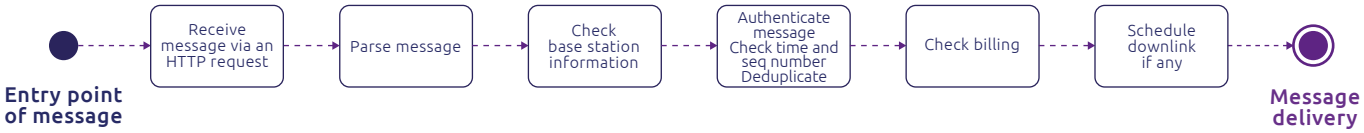

Figure 2: Uplink message processing

In case of a bi-directional communication, the Core Network builds the response, authenticates it and evaluates the best BS to convey this answer. Some whitening and error correction codes are also involved. The following figure shows the Sigfox Core Network process used to send this response to the device.

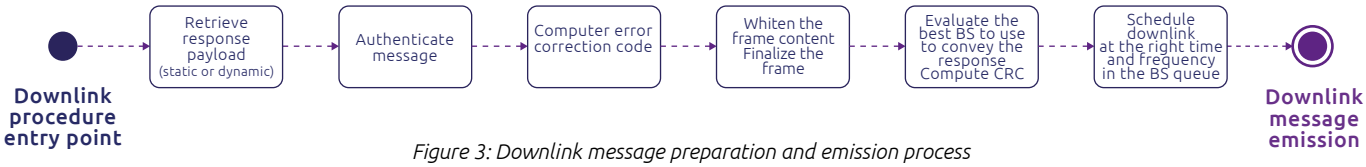

Figure 3: Downlink message preparation and emission process

The emission is made within a timeframe starting after a fixed time following the last uplink message emission. The device will be listening during this Rx window for retrieving this response at a frequency deduced from the uplink message frequency. The figure below shows the different steps for a device to receive a message and to deliver it to the application.

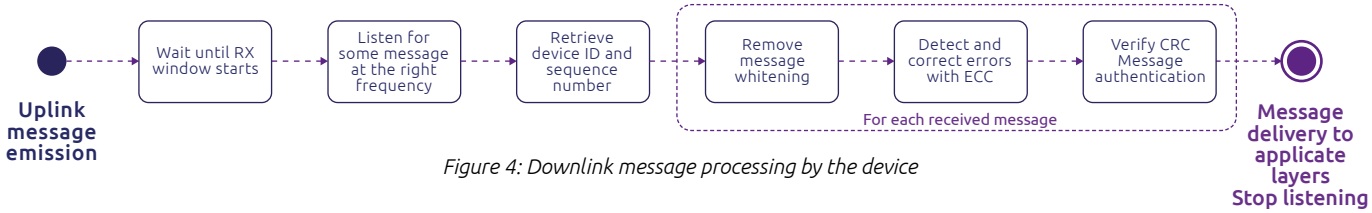

Figure 4: Downlink message processing by the device

2.2 Security needs relating to devices

After having described the system behavior in the first section, we can now focus on the security requirements relating to devices.

2.2.1 What are the security mechanisms defined by the protocol?

The Sigfox protocol provides mechanisms to:

- Authenticate the message: the device is identified by a unique identifier (the device ID) present in the message. Authenticating the message is equivalent to:
  • ensuring that the message has been generated and sent by the device with the ID claimed in the message;
  • checking that the ID is the one of a device known by the system and authorized to communicate on Sigfox network.

- Ensure message integrity: if a message is listened to by an eavesdropper, ensure that any modification can be detected and rejected by the Sigfox network.

- Ensure that a message cannot be replayed: if a message is intercepted by an eavesdropper, ensure that any re-emission of the same message will be discarded by the Sigfox network.

- Optionally provide applicative payload confidentiality: if the customer subscribes to this option, the payload is encrypted from the device to the Sigfox cloud.

The Sigfox protocol **does not** provide mechanisms to:

- Ensure transport channel confidentiality: the radio channel between the device and the base station is not ciphered.

- Ensure applicative payload confidentiality: if the application provider has not subscribed to the Sigfox payload encryption service, the application provider can design the application (and then the device) to cipher the data conveyed by Sigfox frames if required.

2.2.2 How does this work?

Authentification and integrity

Message Authentication Code (MAC)

To guarantee that the message has been sent by the device identified in the message, a MAC (Message Authentication Code) is used.

The **MAC** provides both authentication and integrity evidence to the receiver. A **MAC** generation algorithm is an algorithm that takes as input:

- the message that will be sent and needs authentication (or a part of it);

- a secret key that is shared between the sender and the receiver. This secret keyis generally called the Network Authentication Key (**NAK**).

Then, a cryptographic algorithm will generate a cryptographic token from these inputs. This algorithm must be secure to avoid:

- being able to forge a valid message-tag pair where the tag has not been generated by the sender (i.e., the value must not be predictable);

- having a negligible probability that two different messages will produce the same tag (collision).

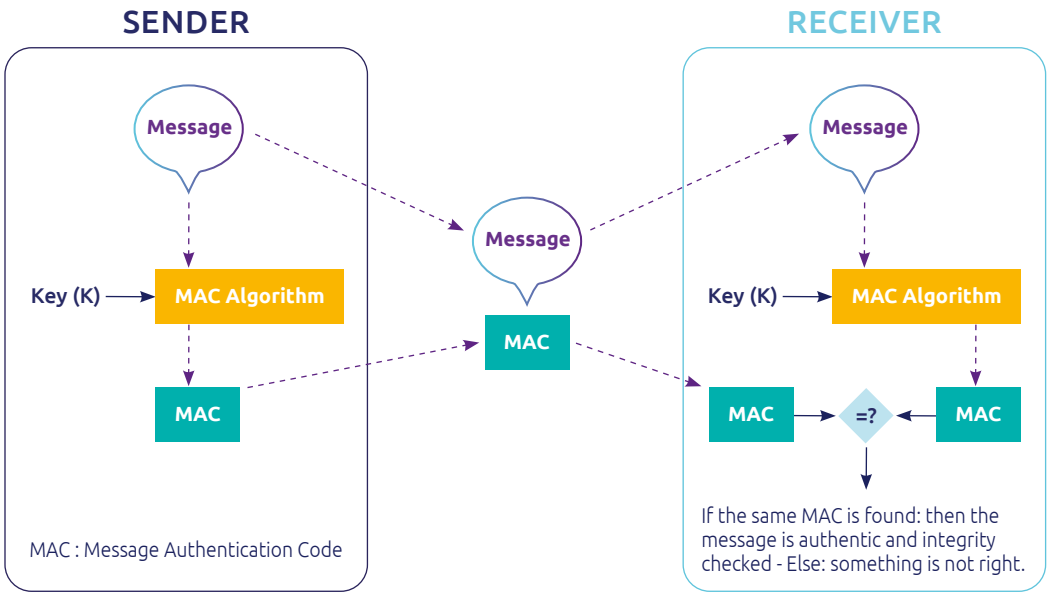

Figure 5: MAC principle (source Wikipedia)

Note that this process uses symmetric cryptography (the key used to generate the MAC is the same as the one used to verify it, the cryptographic algorithm involved is AES-128).

Anti-replay

To prevent an eavesdropper from replaying a message protected by the MAC, a sequence number (SEQ) is present in the message. This sequence number is incremented by the device each time a message is sent to the cloud.

The Sigfox Core Network stores the latest sequence number value sent by the device and discards any message with an invalid sequence number (lesser, equal or not in a specific window above the last value).

As the sequence number value is taken into account in the MAC computation, it is not possible to modify a previous message and change the sequence number. If the same sequence number is re-used, the server will discard the message.

Payload encryption service

The payload encryption service is a service that can be subscribed by the application provider. In this case, Sigfox is trusted by the customer to:

- encrypt the payload in the Sigfox protocol stack in the device (this protocol stack is delivered as a library to the module makers);
- decrypt this payload in the Sigfox Core Network;
- deliver the clear payload via a secured callback to the application provider infra-structure.

The algorithm used is the AES-128 in mode CTR, acting as a stream cipher for datagrams. The following picture explains its principles.

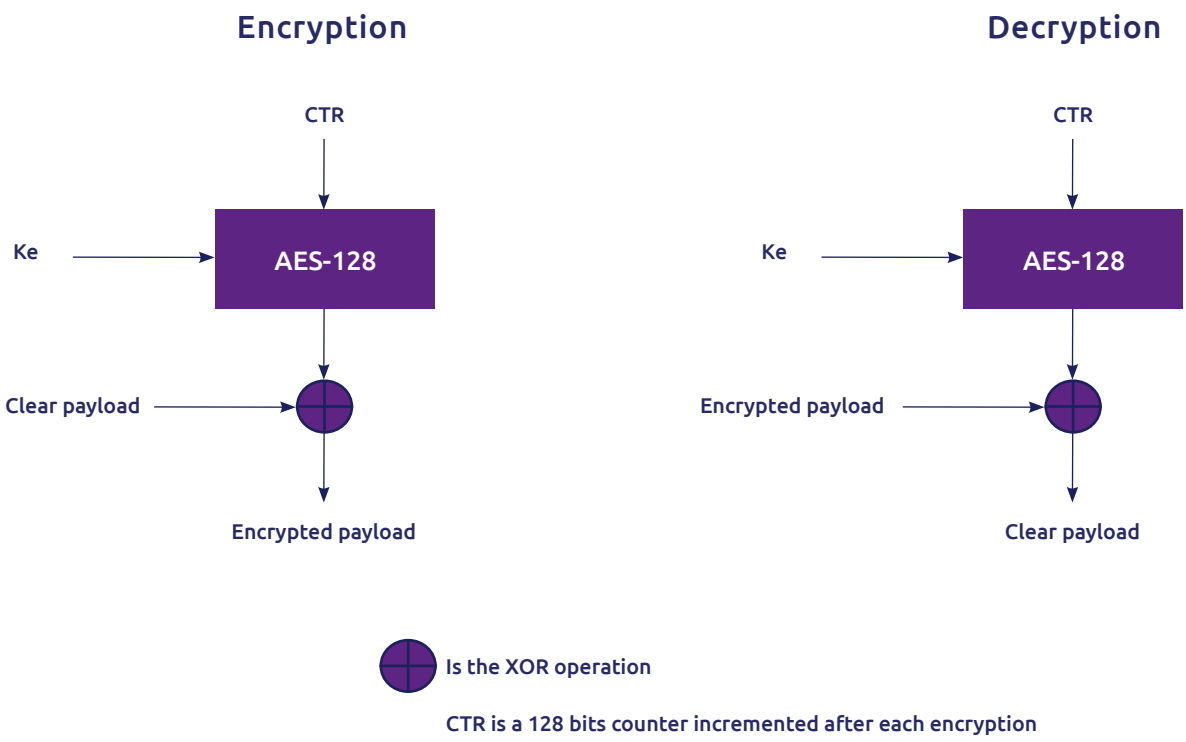

Figure 6: AES CTR encryption and decryption

2.2.3 Sensitive assets to be stored in the device

The mechanisms described above rely on sensitive data:

- the **NAK** (Network Authentication Key) which allows the device to compute the MAC value used by the server to authenticate the message;
- the **device ID** which allows the cloud to identify the device, to retrieve the NAK and the counter SEQ values to decide if the message is valid;
- the **sequence number SEQ** value must be valid and present so the message can get accepted by the server;
- the **encryption key Ke** which is derived from the NAK and allows encrypting the messages' payloads;
- the **CTR encryption counter** which is a payload encryption parameter.

3 Risks of compromised Device Sensitive Assets

In this section we go over the risks that arise when these sensitive assets are compromised. There are two classes of risks:

- the risks affecting the Application;
- the risks affecting the Sigfox network.

3.1 Risks affecting the Application

As the device ID and the counter SEQ values are in clear in the message, they can be easily retrieved without any access to the device. However, changing these values in the device will result in preventing the device to communicate with the server (all the messages could be discarded) or some messages replay (SEQ alteration).

The NAK must not only be protected against modification (as it would have the same consequences as the device ID and SEQ modifications) but also against reading. Indeed, if someone knows this key, they will be able to forge some messages that will be accepted by the server. The risks are:

- loading Sigfox network and application providers with meaningless messages;
- sending false information to influence the behavior of the service.

When the device can perform payload encryption, the encryption key **Ke** and the encryption counter **CTR** must be protected in the Sigfox Ready device. Indeed, if one of these values is altered, the decryption of the payload will be incorrect, and will lead to a failed authentication server side and the data will be discarded and not delivered to the customer.

Moreover, the disclosure of these two parameters results in the possibility to decrypt messages sent over-the-air, breaking the customer's data confidentiality.
The following table sums up the risks:

Parameter	Action	Risk
device ID	Alteration in the device	Denial of device connectivity
Sequence counter	Alteration in the device	Denial of device connectivity Loss of applicative data
Network Authentication Key (NAK)	Alteration in the device	Denial of device connectivity
Network Authentication Key (NAK)	Disclosure	Device cloning, identity theft Fake message injection
Encryption Key Ke	Alteration in the device	Loss of applicative data
Encryption Key Ke	Disclosure	Leak of sensitive applicative data
CTR	Alteration in the device	Loss of applicative data

3.2 Risks affecting the Sigfox network

Since device sensitive assets are specific to said device, whenever a device is compromised, the direct impacts are limited to this device and do not affect other devices. In this sense, compromising one device does not affect the Sigfox network.

However, let's look at two scenarios of potential attacks on the Sigfox network:

- a massive leak of device sensitive assets leading to a large number of devices being compromised;
- the use of compromised devices to conduct denial of service attacks on the network where a large number of authentic messages are fed to the Sigfox network through the radio link.

In the first scenario, an attacker could use the compromised device sensitive assets to generate authentic (but forged) messages that would be transmitted over the radio link. This would deny device connectivity for a large number of devices and affect the credibility of the Sigfox service.

The second scenario is similar in the sense that the attacker generates forged messages that are transmitted over the radio link. The difference is that the goal is to overload the Network resources in order to deny service to uncompromised devices.
This scenario calls for two remarks:

- this attack does not require that the attacking messages are authentic since the core network resources are essentially the same to process authentic or forged messages;

- it is a highly unrealistic scenario. The low bitrate of the Sigfox radio link and the capacity of base stations limit the number of messages that can be fed into the network through any base station.

As a conclusion, compromising device sensitive assets impacts essentially the compromised devices. The Sigfox network will be essentially unaffected. This potential impact is limited to reputation.

4 Compromising scenarios

In this section we discuss the main scenarios that will lead to the various sensitive assets being compromised.

4.1 Remote access to the device

Since devices cannot be accessed from the internet through the Sigfox network, there is no possibility to remotely access the devices and read sensitive assets or modify their firmware.
This, however, is possible when the device has an alternative connectivity such as Wi-Fi, Bluetooth or cellular. This alternative connectivity could be used to attack devices and install rogue software.

4.2 Physical access to the device

In some use cases, the device is not readily accessible to attackers. For example, if the device is part of an alarm system, it will most probably fulfil its service if an attacker tries to access it.

In many use cases, however, the devices are left unattended and may be accessible to attackers. Such devices could be compromised by:

- **destruction:** the sensitive assets are not compromised, but the service is denied;
- **reverse engineering / hacking:** depending on the level of security designed in the device, this scenario may be very simple, complex or almost impossible to achieve. In the simpler cases, the attacker could access the non-volatile memory of the device and directly retrieve the sensitive assets. In more secure cases, the attack may require reverse engineering or even specialized equipment.

In such attacks, one must bear in mind that even if the initial attack is complex, replicating the attack could massively compromise the devices. However, this is mitigated by the fact that a physical access to each device is necessary to compromise it. Accessing a huge number of devices can be difficult and expensive.

4.3 Access to assets during provisioning / manufacturing

Regardless of the security designed in the devices, attack scenarios may involve activity in the asset provisioning chain or during manufacturing. Such attacks could involve the theft of provisioning files and associated encryption keys. They could also involve the theft of credentials to IT systems involved in the provisioning process.

4.4 Eavesdropping of the radio link

The radio link can be listened to by anyone with the proper radio equipment. As we have seen, eavesdropping does not allow to forge or replay messages.

Also, due to the low rate of messages transmission by devices, it is essentially impossible to infer the NAK of a device by listening to the radio traffic. Indeed, this key is an AES-128 key and can take 2128 possible values. With such huge numbers, there is no practical attack on AES-128 by knowing plain/ciphered couples of data. But even if the required CPU means were available, this low rate would not allow building the required data-set for the device through the air interface.

Eavesdropping the radio link, however, allows an attacker to learn the payload data, unless this payload has been encrypted, or if the payload encryption algorithm has not been correctly designed.

5 What are the solutions?

Some solutions exist to prevent the least sophisticated attacks. Indeed, the level of security to apply is always a tradeoff between the cost of the security mechanisms, the level of threat and the cost (or impacts) of an exploit. The main objective is to make the attack more expensive than what can be earned by compromising the device.

This section describes a set of available security solutions that a customer can (or should) use.

5.1 Security assessment

Securing a device is not an easy task, especially when the device must be cheap and made with simple components. In order to ensure that the basic attacks are prevented and that standard best practices are followed, Sigfox customers can request a security assessment from referenced security specialists.

These partners will first perform an assessment of the device's security before suggesting updates to fix potential vulnerabilities that may have been identified. Different levels of assessments are proposed, from checking that the best practices are followed to testing complex attack scenarios requiring professional equipment.
For some critical applications, it is also possible to request some consultancy from day one to have a completely secured service. Moreover, with the support of such companies, it will be possible to be guided and select the most relevant solutions amongst those listed in the next sections.

5.2 Secure provisioning of assets

Sigfox delivers credentials to be loaded in Sigfox Ready devices to device (or modules) makers. As explained earlier, this provisioning link can result in a leakage of all keys for a specific production batch. In case the breach is not detected, this can even apply to several batches.

It is then crucial to secure this channel. Encrypted files containing the credentials are provided to the devices makers via the Sigfox portal. The device makers shall ensure the security of the key used to decrypt the file.

In order to get an optimal security level for this provisioning link, Sigfox will progressively introduce physical security measures to ensure that the credentials are safely transmitted to the factory.

Finally, it is also important that a strict security process is in place to guarantee that the credentials are kept confidential once in the factory. The use of an HSM (see next section) or the physical token provided by Sigfox will prevent external or internal hacking.

5.3 HSM in factory

An HSM (Hardware Security Module) is a secured server or a PCI card that allows to store sensitive keys. These HSMs will detect any intrusion attempt and automatically remove the secret keys they embed.

With such an equipment in factory, it is possible to compute the keys from a secret key (called Master Key – MK – provided by Sigfox and provisioned in the HSM via a key ceremony) and public data. Only the public data are transmitted to the device makers, ensuring that even in case of a successful attack on the provisioning channel, only public data will be disclosed. This process is called key diversification.

Sigfox will strengthen the promotion of this operational process as soon as the volume of produced devices becomes significant.

5.4 MCU with security features

Once loaded into the device, the credentials become vulnerable (again). Indeed, they must be stored in non-volatile memory and might be easily accessible to someone who has physical access to the device.

Micro-controllers could embed security features like dedicated memory for key storage, executable only memory, tamper-detection…
Such micro-controllers can be used in point of sale (POS) devices and provide a first response to trivial attacks.

5.5 Secure Element

The highest security level for protecting the device credentials is provided by the Secure Element (SE), a tamper-resistant chip conceived to resist the most complex attacks. This type of chips is used in credit cards, SIM cards, biometric passports…

Several SE makers have worked with Sigfox to introducea Sigfox-compliant SE in 2017. ST Microelectronics, Trusted Objects, Wisekey and Safran Identity & Security already announced Secure Elements Sigfox compliant for 2017.

5.6 Physical Unclonable Functions (PUF)

Some algorithms available as piece of software use the intrinsic characteristics of hardware components (like delays or uninitialized SRAM value) to compute metrics specific to each device (even of the same model). These metrics are used to compute keys that can help protecting the credentials in the device's non-volatile memory.

As these keys are computed and not stored, it is quite difficult for an attacker to reverse-engineer the device to retrieve them and then the credentials.

Sigfox is currently reviewing such a solution with a partner.

5.7 Payload encryption

Sigfox offers a payload encryptions solution. This solution results from a joint work with a cryptography-specialized research institute (CEA-LETI). It consists of a robust payload encryption algorithm that does not change the size of the payload when it is encrypted. This encryption uses AES-128 in CTR mode.

When using this option, the customer shall accept that Sigfox performs the payload decryption prior to delivering the data. In case the customer wants an end-to-end confidentiality (from the device to the customer's cloud application), it must implement its own encryption mechanism. In this case, Sigfox will not see the data in clear and will deliver it encrypted to the customer's application.

In both cases, encryption will prevent an eavesdropper to have access to sensitive data in plain text.

6 Conclusion

As explained in this document, devices getting compromised can generate huge impacts on customer business or infrastructures.

These damages can be:

- the disclosure of sensitive data;
- the injection of fake data in the customer applications, making customers take some bad decisions, which could be dangerous for their businesses, infrastructures, goods or data;
- a bad reputation in the market, resulting in a lower revenue for a potentially long period.

For Sigfox, the fact that one or several devices are compromised leads mainly to an alteration of its image as a secure IoT network provider, even if securing devices is not its responsibility.

This is why the customers should strongly consider being guided for making their devices and application more secure and using one or several of the solutions described in this document.

Sigfox is committed to protecting its network and strengthening its security to make it one of the safest, but also to explore new techniques, exploiting big data and machine learning power to detect devices or data flows anomalies and to take relevant protection measures (notification to the customer that a device has a suspicious behavior, data flows disconnection or redirection, etc.).

This would close the loop, the high volume of data generated by the IoT helping securing this new ecosystem, acting as a self-healing system. However, all the actors still have to take their responsibilities and to secure their own assets, for everybody's peace of mind.

+33 (0)5 82 08 07 10
Bâtiment E-volution
425, rue Jean Rostand
31670 Labrège – France
sigfox.com

sigfox