Sigfox
Technical Overview

May 2017

Table of Contents

1 Introduction

This document provides a general overview Sigfox technology and Sigfox global network.

It first introduces the principles of Sigfox technology in terms of communication between the object and the network. It details the competitive advantages of this technology to address the IoT market.

The second section describes the architecture of the Sigfox network with its different components, their roles and responsibilities.

The third section describes the mechanisms and processes in place within Sigfox for securing customer data as well as the network infrastructure from base stations to core network components.

The last section presents the different features provided by Sigfox to evaluate service coverage.

How to develop Sigfox-enabled solutions?

Go to our dedicated website for device makers: build.sigfox.com
You will discover how to easily integrate Sigfox technology in a device and perform integration with any IT platform.

List of acronyms

ACRONYM	DEFINITION
AES	Advanced encryption standard
API	Application programming interface
BS	Base station
BSS	Business support system
CaaS	Connectivity as a service
CPA	Channel partner agreement
CRA	Central registration authority
GUI	Graphical user interface
IoT	Internet of things
ISM	Industrial, scientific and medical
IT	Information technology
KPI	Key performance indicator
LPWAN	Low power wide area network
MAC	Message authentication code
NAK	Network authentication key
NIP	Network infrastructure provider
NOC	Network operation centre
OSS	Operation support system
OTA	Over the air
PAC	Porting authorisation code
RF	Radio frequency
RSSI	Received signal strenght indicator
SLA	Service level agreement
SLO	Service level objective
SO	Sigfox operator
SSL	Secure socket layer
TAP	Transfox access Point (BS)
TPM	Trusted platform module
TCO	Total cost of operation
UNB	Ultra-narrow band
VPN	Virtual private network

2 Sigfox positioning

● **It's about connecting the unconnected!**

Many of tomorrow's great ideas are technically possible today. They are just constrained by cost and energy issues. The reality is that small inexpensive objects simply do not have enough power to communicate with large mobile networks. This is why Sigfox pioneered low power device-to-cloud connectivity to complement high band-width solutions.

Sigfox low powered connectivity solutions not only improve existing business cases but also enable a new range of opportunities for businesses across all industries. There are no limits to what can be acheived.
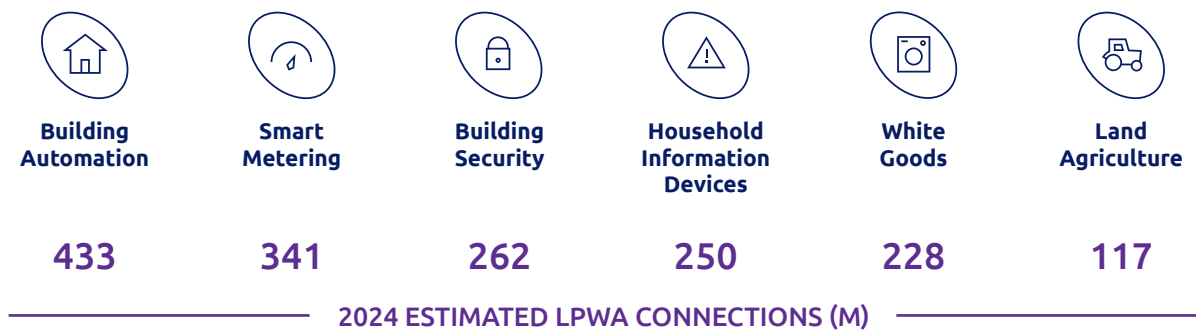
Building Automation	Smart Metering	Building Security	Household Information Devices	White Goods	Land Agriculture
433	341	262	250	228	117

2024 ESTIMATED LPWA CONNECTIONS (M)

Figure 1: Whatever the industry, Sigfox matters!

● **Sigfox is moving the world forward**

Through its global LPWA network and rich ecosystem of expert partners, Sigfox delivers out-of-the box, two-way, secured communication services to unlock the true potential of the Internet of Things (IoT).

Sigfox provides a standard way of collecting data from sensors and devices with a single, standard-based set of APIs. Besides, the Sigfox disruptive technology complements traditional cellular M2M by enabling global, ubiquitous, ultra-long battery life solutions at the lowest cost.

Sigfox has great potential as a secondary connectivity solution to enable lower battery consumption and better user experience.

Sigfox provides the network, the technology and the expert ecosystem, which are necessary to help companies and organizations make the most of their IoT ambitions.

3 Technology principles

This chapter introduces the main principles of Sigfox technology in order to demonstrate its positioning and its competitive advantages.

3.1 Ultra-Narrow Band (UNB)

Sigfox is using 192KHz of the publicly available band to exchange messages over the air. The modulation is Ultra-Narrow band. Each message is 100 Hz wide and transferred with a data rate of 100 or 600 bits per second depending on the region.

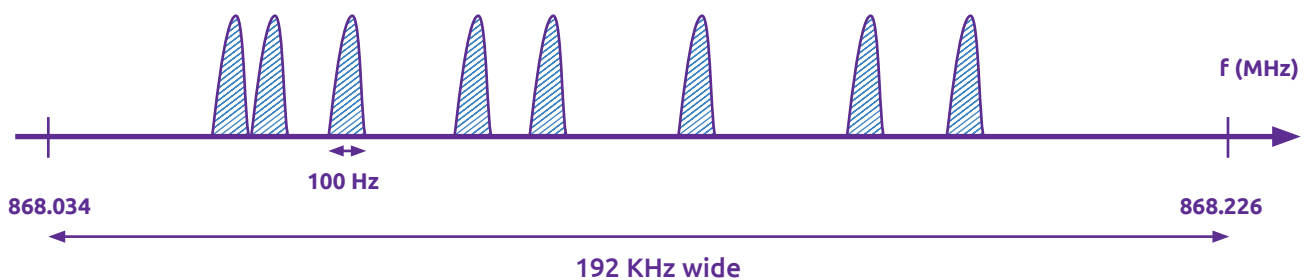*Figure 2: Sigfox technology based on Ultra-Narrow Band.*

This is what enables the Sigfox base stations to communicate over long distances without being impacted by the noise.

The band used depends on the location:

- **in Europe,** for example, the band used is between 868 and 868.2 MHz;

- **in the rest of the world,** the band used is between 902 and 928 MHz with restrictions according to local regulations.

3.2 Random access

The random access is a key feature to achieve a high quality of service. The transmission is unsynchronized between the network and the device. The device emits a message on a random frequency and then sends 2 replicas on different frequencies and time, which is called "time and frequency diversity".
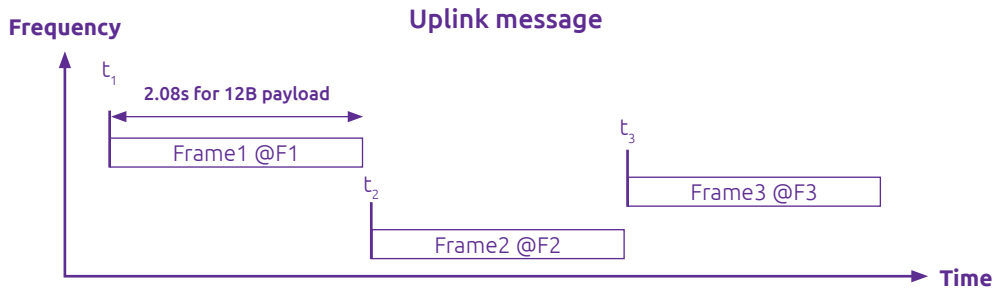

Figure 3: Frequency hopping on replicas.

A message with a 12-byte payload takes 2.08s over the air with a rate of 100 bps.

The Sigfox base stations monitor the full 192 kHz spectrum and look for UNB signals to demodulate.

3.3 Cooperative reception

The principle of the cooperative reception is that an object is not attached to a specific base station unlike cellular protocols. The emited message is received by any base stations that are nearby and on average the number of base stations is 3. This is called "spatial diversity".

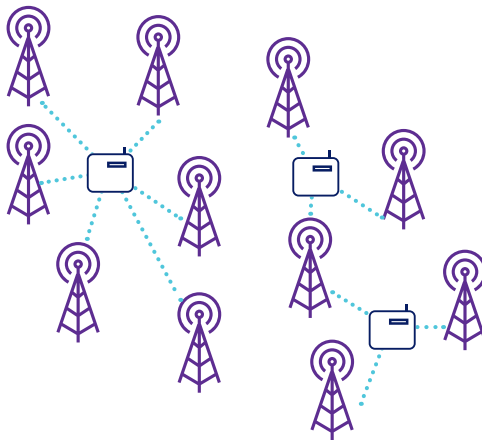

Figure 4: Message reception by multiple Sigfox base stations

Spatial diversity coupled with the time and frequency diversity of the repetitions are the main factors behind the high quality of service of the Sigfox network.

3.4 Small messages

In order to address the cost and autonomy constraints of remote objects, Sigfox has designed a communication protocol for small messages. The message size goes from 0 to 12 bytes. A 12-byte payload is enough to transfer sensor data, the status of an event like an alert, GPS coordinates or even application data.

We have listed some payload size examples:

GPS coordinates ··············▶ 6 bytes

Temperature ··············▶ 2 bytes

Speed reporting ··············▶ 1 byte

Object status ··············▶ 1 byte

«Keep alive» payload ··········▶ 0 byte

The regulation in Europe states that we can occupy the public band for 1% of the time. This translates into 6 12-byte messages per hour or 140 messages per day. While the regulation differs in other regions, the Sigfox commercial offer remains the same at the moment.

For downlink messages, the size of the payload is static: 8 bytes. Again, a lot of information can be transferred on 8 bytes. This is enough for triggering an action, managing a device or setting application parameters remotely.

The duty cycle for the base station is 10% that guarantees 4 downlink messages per device per day. If there are extra resources left, the device can receive more.

3.5 Bi-directional

The downlink message is initiated by the object. There is a delay of 20 seconds between the first frame transmitted and the reception window that lasts for 25 seconds maximum.
The downlink frequency is the frequency of the first uplink message plus a known delta.

4 Key features of the network

This section addresses the main characteristics of the Sigfox network itself in terms of architecture & performances.

4.1 Network architecture overview

This chapter is an introduction to the Sigfox network with a high-level description of its different components.
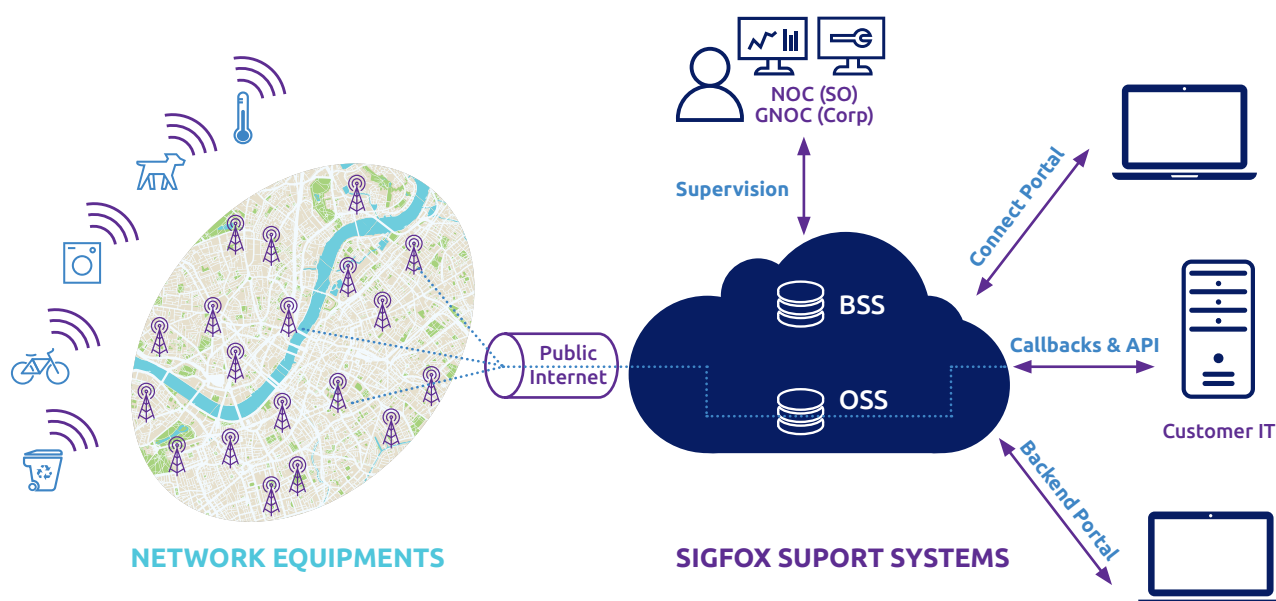

Figure 5: High-level architecture of the Sigfox network

The Sigfox network has a horizontal and thin architecture composed of 2 main layers.

🚀 The Network Equipment layer consists essentially of bases stations (and other elements e.g. antennas) in charge of receiving messages from devices and transferring them to the Sigfox Support Systems.

🚀 The Sigfox Support System is the second layer constituting the core network in charge of processing the messages and send them through callbacks to the customer system. This layer provides as well the entry point to the different actors of the eco-system (Sigfox, Sigfox operators, channels and end-customers) to interact with the system through web care interfaces or APIs. This layer also includes modules & features which are essential to ensure the deployment, the operation and the monitoring of the network such as the Business Support System for ordering & billing, the Radio Planning supporting the deployment of the network, the monitoring to ensure the good working of the network. Besides, this layer includes repository and tools to analyze the data collected or generated by the network.

As mentioned in the figure above, the link between the two layers is ensured by the public Internet but secured with VPN connection.

The following chapters describe the different components of those two layers of the Sigfox network.

4.2 Flat network architecture

The flat architecture of Sigfox is key to minimize both CAPEX and OPEX. The Sigfox Software Defined Radio (SDR) helps to overcome high hardware costs for base stations. No special hardware has been used but instead a software algorithm to handle demodulation in an effective manner. It reduces significantly the Total Cost of Operation (TCO).
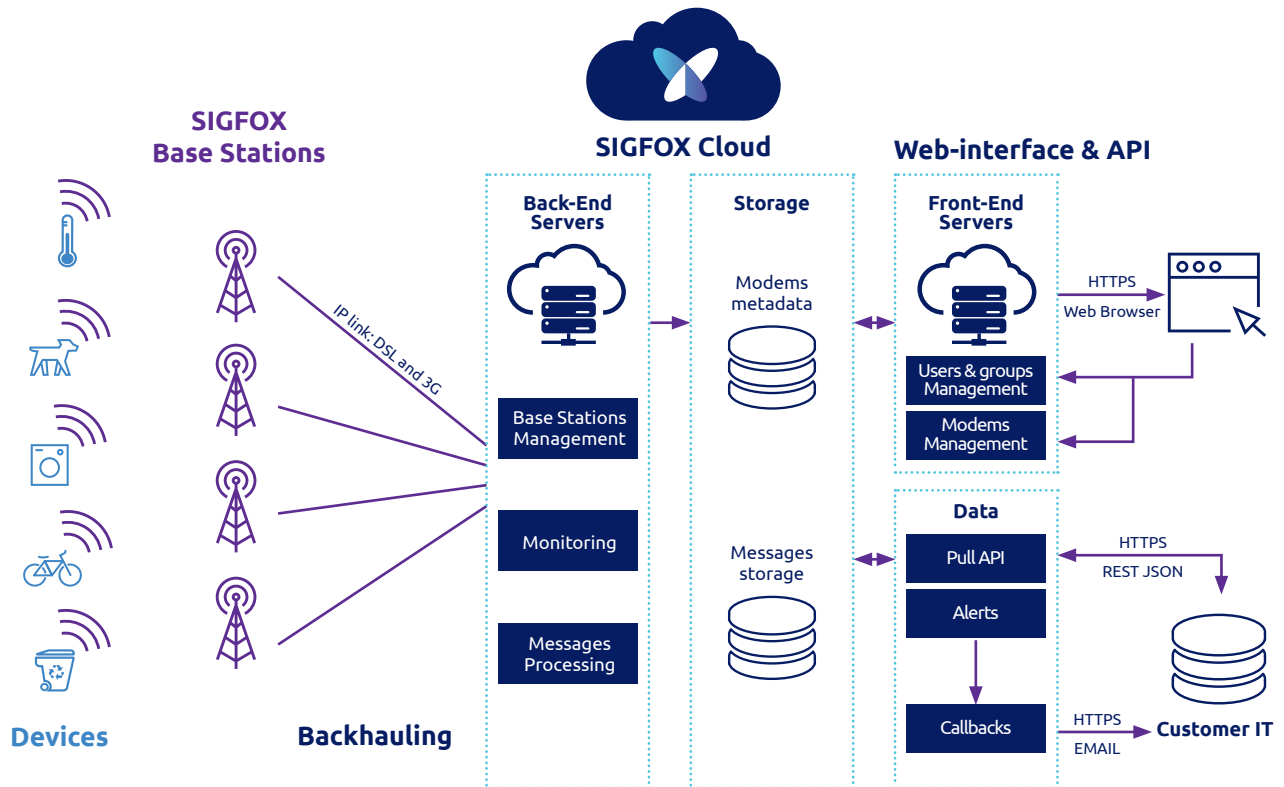

Figure 6: Flat architecture

The data is sent over the air to the base stations, then goes through the backhaul. The backhaul generally uses DSL connectivity and 3G or 4G as a back-up. When one of the two is not available, satellite connectivity can be used as an alternative back-up technology.

The back-end handles message processing. There are potentially lots of replicates of the same message that arrive on the core network but only one should be stored. The core network servers also monitor the status of the network and manages the base stations globally.

The network infrastructure also stores the messages in two locations: the metadata can be used for building services on one hand and the customers' messages so that customers can retrieve them later on the other hand.

Finally, the web interface and the API allow customers to access their messages. They can either access the platform through their web browser or use a REST API to synchronize them with their IT system and push downlink messages to the device.

4.3 High network capacity

The capacity of the network is high, enabling Sigfox to scale for the billions of objects. The massive capacity of the infrastructure of the Sigfox network is the result of the factors described earlier:

- ultra-narrow band modulation has the benefit of being spectrum efficient and resistant to interferers as all of the energy is concentrated into a very small bandwidth;
- frequency and time diversity introduced by the random access;
- spatial diversity due to the overlapping network cells.

UNB + Frequency & Time diversity + Spatial diversity = Massive capacity + High Quality of Service
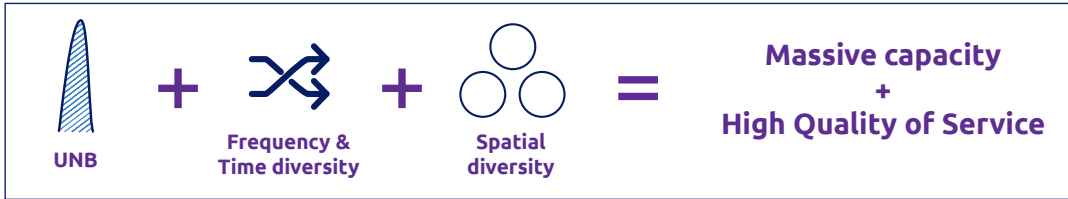
Figure 7: Combination of Sigfox specificities

The capacity is the same regardless of the radio link, whereas other networks have a decreasing capacity as the radio link quality gets worse.

Figure 8: Capacity sustaining regardless of the quality of the radio link

If the targeted quality of service is 99,99%, the load on the base station shall not be higher than 14%. In other words, with close to 270 objects communicating in parallel, the probability of collisions gets higher and therefore the probability of losing a message increases to more than 0.01%.
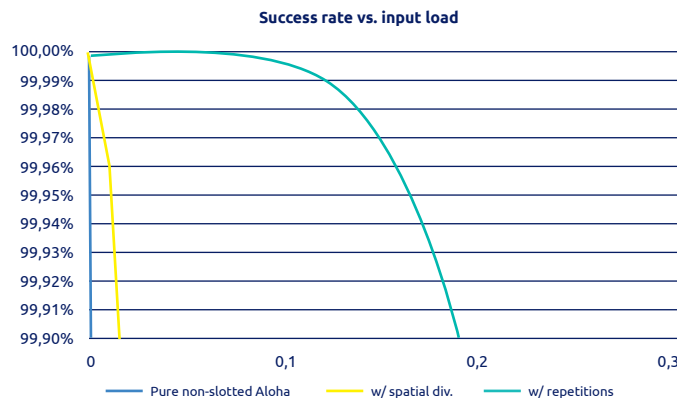

Figure 9: Limited impacts of the load on the quality of service thanks to repetitions

4.4 High energy efficiency

The high energy efficiency enabled by Sigfox technology also relies on the Sigfox semiconductor partners as their chips consume from 10mA to 50mA in transmission – depending on the partner and chip used.

These values are applicable in Europe where the output power is 14dB but the current is higher in the US where 22dB are required. However, the time on air is six times inferior therefore the battery life is about the same.
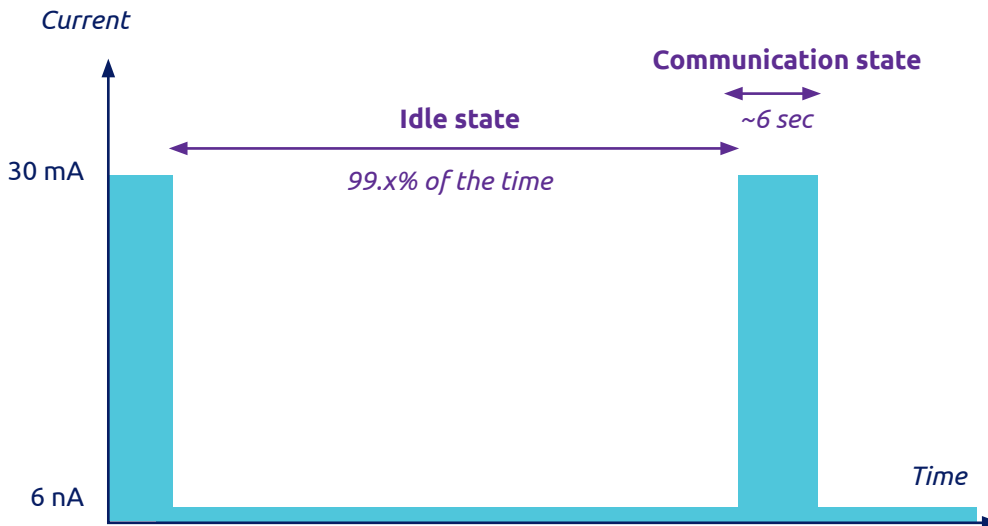

Figure 10: Low idle consumption increasing the battery life

There are two more factors explaining the long battery life with Sigfox.

- No pairing is required, which means that no synchronization messages are exchanged between the object and the base station before transmitting the data. This is a big advantage compared to other technologies which all include those additional steps.

- Also the idle consumption is very low, often a few nanoamperes, which makes it almost negligible.

4.5 Long range

The main competitive advantage of the Sigfox technology is on the deployment with a large coverage and a limited number of base stations:

- for a given output power, the range of the radio frequency (RF) link is determined by the data rate, i.e. a lower rate provides a longer range;

- the second factor is the link budget, sum of the base station sensitivity & the output power of the object;

- highly depends on the topography;

- good indoor coverage due to the use of sub GHz band.

15

The long range of the base stations enables Sigfox to deploy a nationwide network at a minimum cost. The long range is due to the low data rate, 100 bits per second, the output power of the object and the sensitivity of the base station.

In terms of radio frequency range, Sigfox uses a metric called the link budget:

🛰 the link budget is the sum of the sensitivity of the base station, the antenna gains and the output power on the object's side;

🛰 it ends up with a slightly higher budget link in the ETSI zone, resulting in larger cells;

🛰 the good indoor coverage of Sigfox is due to the use of the sub GHz band. Other technologies claiming a higher budget link and using 2.4 GHz, will suffer for indoor use cases.

4.6 Resilience to interferers

Sigfox technology presents unique anti-jamming capabilities due to UNB intrinsic ruggedness coupled with spatial diversity of the base stations (+20 dB).

For the technical reasons as mentioned above, UNB is extremely robust in an environment with other signals, including spread spectrum signals. However, spread spectrum networks are affected by UNB signals. Ultra Narrow Band is therefore the best choice to operate in the public industrial, scientific and medical (ISM) band.

The high resilience to interferers is key to operate efficiently in the public ISM band.

The best proof of the high resilience to interferers is the capability to transmit despite the presence of jamming signals. Ultra-narrow band modulation has some intrinsic ruggedness because the overlap with the noise is very low. For a message to be received, the signal should be at least 8 dB above the noise floor.
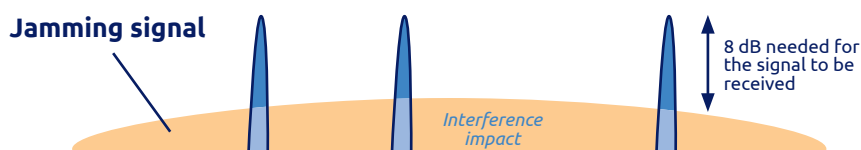

Figure 11: Resilience to interferers provided by UNB

Competing technologies built on spread spectrum modulation are highly impacted by noise because the surface they have in common is much bigger. UNB is the best possible signaling choice to operate in the public ISM band.

4.7 Security by-default

The Sigfox ecosystem integrates the security by-default:

- authentication + integrity + anti-replay on messages propagated on the network;

- cryptography based on Advanced Encryption Standard (AES) with no key OTA transmission;

- payload encryption as an option to ensure the confidentiality of the data;

- isolation of each part of the network and assess the risks so that in case of a hack only a minor segment of the network is impacted.

On the device side, Sigfox had defined three different levels of security. Depending on the use case and its sensitivity, the device maker or the application provider will decide which level to implement:

- medium level – the security credentials are stored in the device;

- high level – the security credentials are stored in a S/W based protected area;

- very high level – the security credentials are stored in a secure element.

The secure element also helps to encrypt the data that is transferred over the network. Only the device and the end-customer know the secret key. The algorithm does not impact the size of the payload. While the message is encrypted, the payload is still 12-bytes long.

Throughout the path of the message, the Sigfox network makes sure that the device ID has not been duplicated. In the case of a corrupted device, a blacklist list mechanism will prevent the communication of this device.

From the start, Sigfox has designed the network with security in mind, separating functions onto several servers. For instance, the server generating IDs has a reinforced security.

5 Security overview

Based on its expertise and its partnerships, Sigfox has applied security by design principles in all the definition steps of its protocol and in the development of its infrastructure.

Furthermore, Sigfox is applying security-by-default principles in all the components it offers to Sigfox users, Sigfox operators, device manufacturers and end-customers.

This encompasses the complete IoT chain including devices, network infrastructure, and cloud-based services:

DEVICE
- Crypto capabilities
- Subscription management
- Device management

DATA
- Data Integrity
- Data Encryption: confidentiality
- Data privacy

RADIO
Protect DATA IN MOTION
- UNB radio robustness
- Authentication & Integrity

CLOUD
Protect DATA IN REST
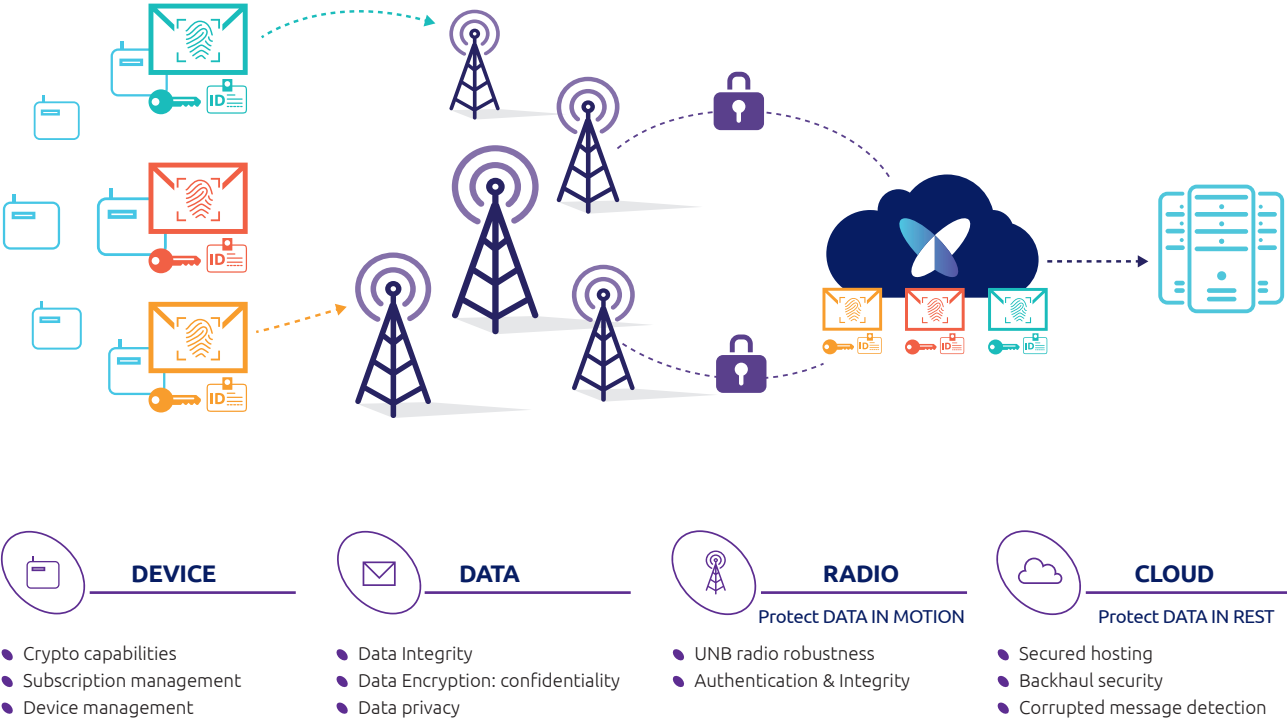- Secured hosting
- Backhaul security
- Corrupted message detection

Figure 12: Security by-design & by-default

A built-in Firewall

Although devices integrating the Sigfox technology are IoT objects, they are not directly connected to the Internet and do not communicate using the Internet protocol. Actually, those devices are not connected to any network or to any base station.

They have a built-in behavior. When this behavior requires that data is transmitted to or received from the Internet, the device will broadcast a radio message. This message is then picked up by several access stations and conveyed to the Sigfox Support System, which in turn delivers it to a predefined destination, typically an IoT application.

If the device requires a response, the IoT application has the opportunity, during a limited time window, to deliver the response to the device through the Sigfox Support System and base stations.

This design implies that devices never have the ability to send data to arbitrary entities via the Internet. They are therefore shielded from the Internet by a very strict firewall.

Security of data in motion

Message authentication and replay avoidance measures are the foundation of data in motion security and are critical to winning trust in the whole ecosystem. The design of the Sigfox protocol provides such features by default. These are completed by an optional anti-eavesdropping measure.

Security of data at rest

Critical data is stored in all entities of the IoT chain from devices storing their authentication key to the Sigfox Support System security assets concerning the network as well as customer data. This implies different security mechanisms within the Sigfox ecosystem as well as best practices and processes ensuring integrity, availability and confidentiality of this data by respecting local regulations.

As the key is unique for each device, the compromising of one device has a very limited impact. Nevertheless, good security practices and secure storage will be implemented by the device designer.

Sigfox has been working with its ecosystem to increase the security level of devices through the adoption of security best practices. In addition, secure elements dedicated to Sigfox devices are now available to provide tamper resistance.

Finally, Sigfox partners with companies specialized in security assessment to help customers with critical applications to achieve the right security level.

Base stations store credentials to communicate with the Sigfox Core Network. State-of-the-art approaches relying on Trusted Platform Module (TPM) secure this entity. Sigfox Core Network stores Sigfox ReadyTM devices' authentication keys as well as traffic metadata. State-of-the-art solutions have been deployed to ensure the integrity, availability and confidentiality of these data. A continuous improvement process has been defined to ensure that Sigfox Core Network is compliant with local regulations.

5.1 Security on message processing

As presented in a previous section, there are different checks done by the global Sigfox ecosystem during the message processing:
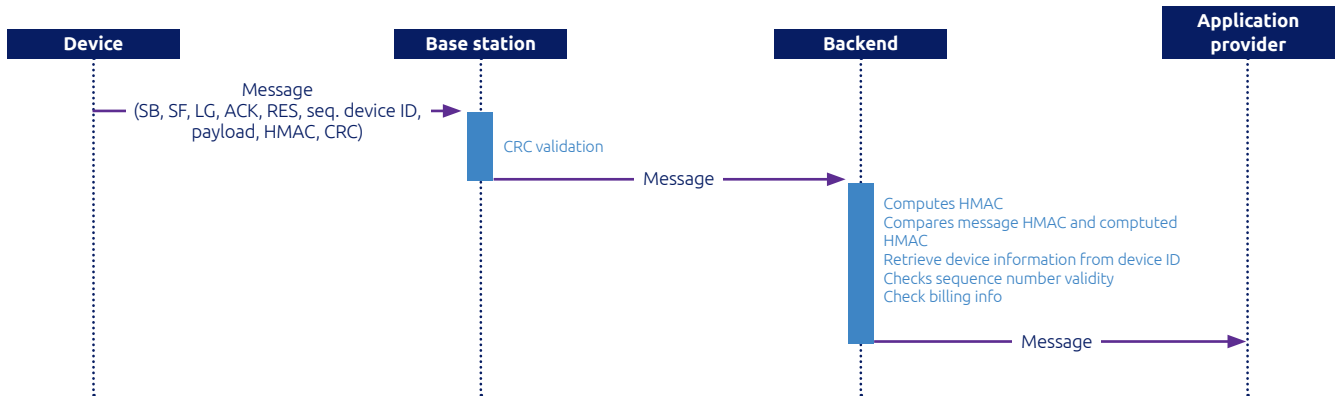

Figure 13: The different checks executed along the uplink message treatment

The following paragraphs detail the different mechanisms put in place.

5.1.1 Sequence number

The sequence number is an anti-replay mechanism (associated with MAC). It is a simple message counter starting from zero to one byte unsigned integer (one month rotation with 140 messages/day).

The sequence number is verified by the Sigfox Support System to detect and discard replay attempts. The integrity of the counter is guaranteed by the message authentication token.

There is a validity window of this sequence number to receive the messages. This range is between (last validated sequence number + 1) and (last validated sequence number + 1 + 3 x the subscription level – corresponding to the maximum number of messages generated by the device by day – with a minimum value of 20).

For example, if the last validated sequence number was 5, the validity window for the next sequence number will be the following according to the subscription level:

- 🛰 if the subscription level is platinum with 140 messages per day, the sequence number shall be between 6 and 426 (6 + 3 x 140);

- 🛰 if the subscription level is one message per day, the sequence number shall be between 6 and 26 (6 + 20) because 3 x 1 messages < 20.

5.1.2   MAC verification

Each device is provisioned with a unique symmetrical authentication key during manufacturing. Each message to be sent or received by the device contains a cryptographic token that is computed based on this authentication key. Verification of the token ensures: the authentication of the sender (the device for an uplink message, or the Sigfox network for a downlink message) and the integrity of the message. In the IT segment, authentication of communications between the Sigfox Core Network and application servers relies on classical Internet approaches such as VPN or HTTPS.

The MAC verification guaranties:

🖋   the integrity – the message is not altered;
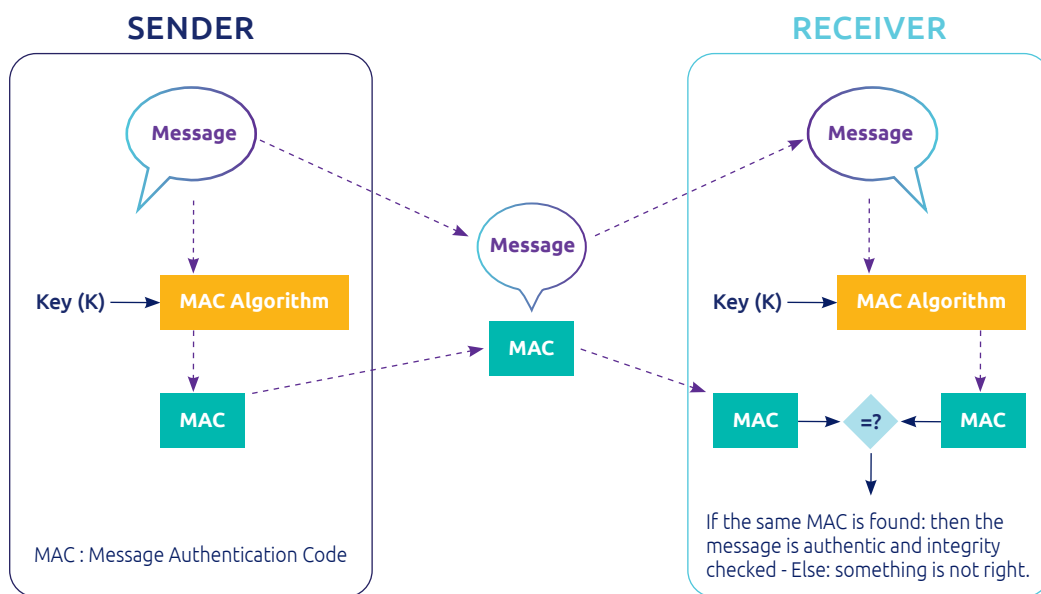
🖋   the authentication of the sender.

Figure 14: MAC verification to check the message integrity and device authentication (source Wikipedia)

As the message contains the sequence number (see previous section), a message cannot be replayed by someone even if it increases the sequence number because the MAC will not correspond.

5.1.3   Message Encryption

By default, data is conveyed over the air without any encryption. However, depending on the application, this data may be very sensitive and its privacy must be guaranteed.

Sigfox gives customers the option to either implement their own end-to-end encryption solutions or to rely on an encryption solution provided by the Sigfox protocol. This encryption solution was specially designed for very short Sigfox messages in collaboration with CEA-LETI. The encryption key is derived from the device key. The encryption will use NAK (device key), sequence counter and rollover counter.

5.2 Security on base station and its communication

A base station can be deployed in a hostile environment even though it contains IP that shall be protected. Sigfox has integrated a TPM in the base station to secure all the keys involved in the different mechanisms securing the base station.

🛰 Nobody can steal Sigfox sensitive software.

🛰 Nobody can alter the base station operating system:
- a secure boot checks its integrity;
- the IMA (Integrity Measurement Architecture) ensured the integrity of the runtime.

🛰 There is a binding between the OS and the hardware:
- the base station can only boot an OS built by Sigfox;
- the OS can only run on a base station hardware.

The communication between the base station and the Sigfox Support System is secured by a VPN preventing any intrusion in the core infrastructure from the base station. The VPN credentials are also protected by the TPM.

5.3 Security on key generation and provisioning

The key generation & provisioning corresponds to the ordering and the provisioning of device credentials (device ID and NAK) into the device (within a secured element, a communication module or SoCs or devices directly).

This process can be executed only if the corresponding manufacturer has successfully passed the certification required by Sigfox to communicate on the network. Depending on the component (module or device), there are different levels of certification.

The process is described hereafter.

🛰 The manufacturer sends an email with a request for a batch of N device ID along with the associated certificate to Sigfox.

🛰 Once the order is validated internally, Sigfox assigns a device ID range to the manufacturer for the given certificate and launches the generation. The Central Registration Authority (CRA) generates a Network Authentication Key (NAK) and a Porting Authorization Code (PAC). The PAC is used later in the process to activate the device. The database is provisioned with the result of the generation.

🛰 The manufacturer retrieves the output files from the CRA:
- a binary file containing (device ID, key) pairs encrypted in AES-ECB;
- a text file containing (device ID, PAC) pairs.

- The manufacturer uses a Sigfox application and a dedicated key delivered by Sigfox to decrypt and load the key and device ID in each module and optionally the initial PAC code.

- The application provider/end-customer receives devices/modules from the manufacturer with their device IDs and their PACs.

- The application provider/end-customer accesses to the web portal of the Operation Support System (OSS) in order to register the device by providing its device ID and its PAC to a Sigfox Operator.

- The OSS checks in the CRA, the device ID and the PAC before generating a new PAC sent back to the application provider/end-customer. This regeneration of the PAC prevents its re-use by another Sigfox Operator.

With this approach, the NAKs are never seen in clear outside the secured execution environment dedicated to cryptographic computation.

5.4 Security on data center

The Sigfox Support System is essentially a cloud-based network. As such, it benefits from proven Internet technologies and suppliers.

- More specifically, the Sigfox Support System is hosted in secured certified data centers. Each rack is secured with biometric protection for physical access.

- Each data center is doubly Internet-attached through different Internet transit providers.

- By design, Sigfox architecture is fully load-balanced and redounded from the core switching to the applicative servers based on virtual machines through double-attached physical servers.

- At the application layer, each component is fully redundant, strongly monitored and fully scalable to support any increase in traffic.

The cloud-based model of Sigfox ensures high availability access to the Sigfox Operational and Business Support Systems service components, decreasing downtime and other operational risks controlled by the Sigfox Service Continuity Plan.

A dedicated solution protects Sigfox data centers against a wide range of denial-of-service cyber-attacks such as denial-of service (DoS), distributed denial-of-service (DDoS), reflective denial-of-service (RDoS), and distributed reflective denial-of service (DRDoS).

This solution, supplied and maintained by our Internet service provider, offers a cloud-based protection service with several scrubbing centers in order to detect and mitigate cyber-attacks against networks and websites. This solution uses proprietary detection and mitigation algorithms matching Sigfox-specific traffic patterns to prevent false positives.

6 Service coverage tools

This chapter presents the different features provided to channel partners to evaluate the service coverage.

6.1 Service coverage public access

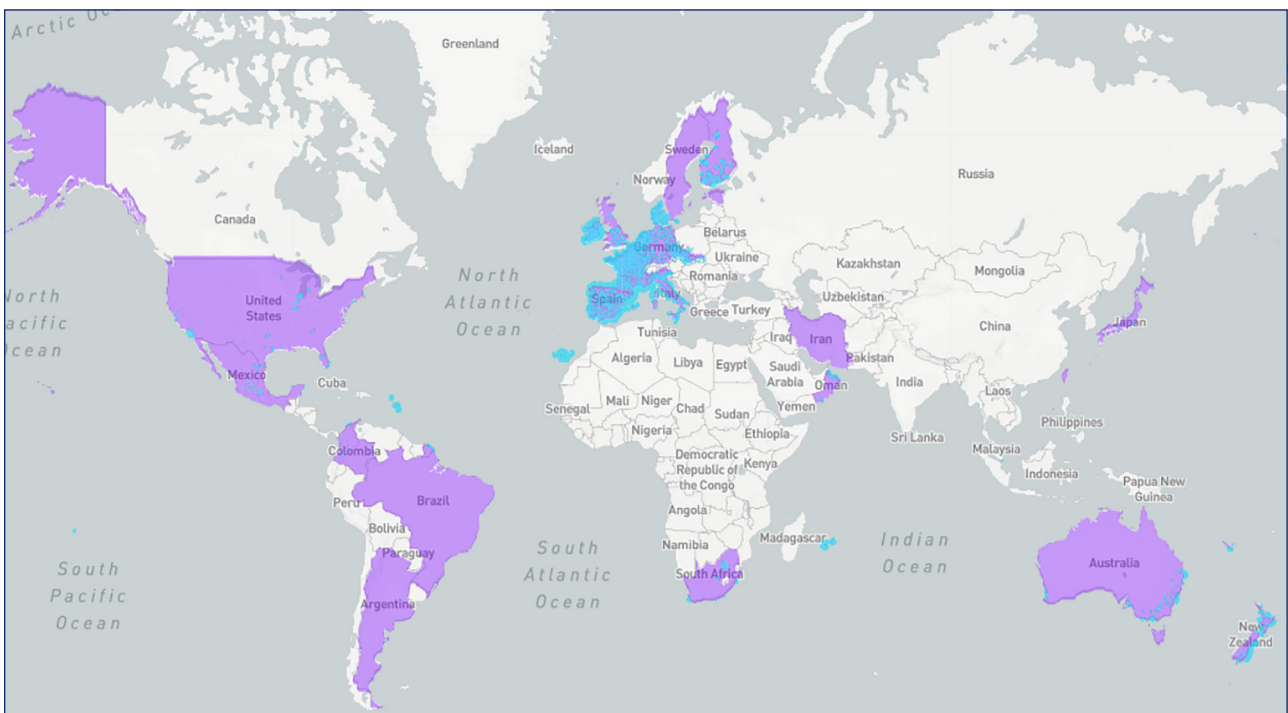A link to a coverage map can be accessed via Sigfox web site: **www.sigfox.com/coverage**

Figure 24: Global coverage map - This map is regularly updated, please check www.sigfox.com/coverage

This map is only a guide and not a guarantee of service level. Coverage estimation based on computer prediction in outdoor location for device class U0 (maximum output power level as defined in SIGFOX Ready™ certification requirements). SIGFOX attempts to provide accurate and complete information through this online coverage estimation tool. However, neither SIGFOX nor its Distributors within the regions covered by this map can guarantee the quality, accuracy or completeness of the information. The coverage estimation tool is for information purposes and is provided «as is» without warranties of any kind, either express or implied. SIGFOX and the relevant Distributors within the regions covered by this map assume no liability for any damages resulting from the use or misuse of the coverage estimation tool.

This is public access and displays the live network coverage as well as the countries being rolled out.

6.2 Service Map

A service map is available in the OSS Portal for Operator and Channels for their territories.

It works as a heat map providing real time coverage information. The user selects the product uplink class and desired radiolink margin to obtain Sigfox service map corresponding to an application:
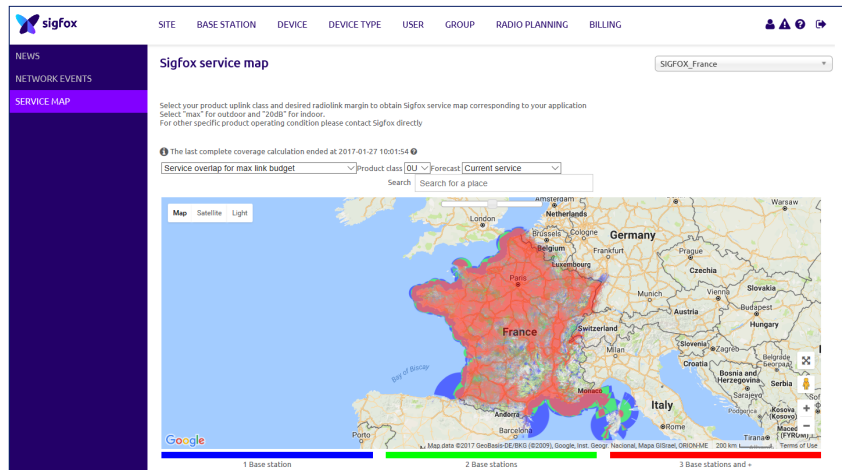

Figure 25: Service map integrated to OSS portal.

6.3 Global Coverage API

A new API is being developed and will be accessible to all OSS Portal users (Operators and Customers).

The aim is to provide the coverage quality of all Sigfox public operators worldwide while being adapted to any application type (penetration, objects…)

The POST request is made with latitude and longitude {lat, long} or with a specific postal address.

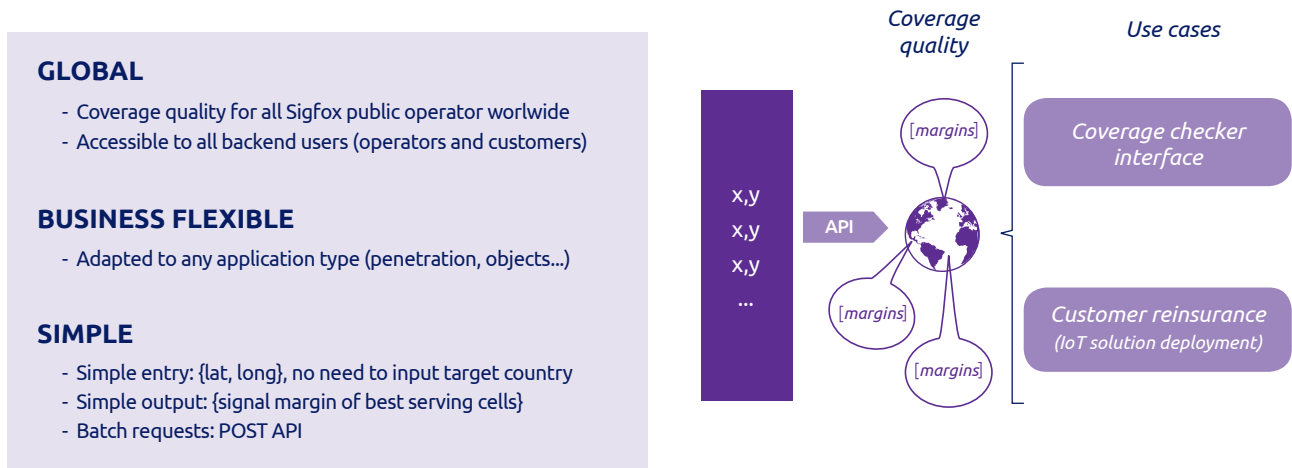The output is simply the signal margin of the best serving cells.

Figure 26: Global coverage API to evaluate the network coverage on different locations

sigfox