sigfox

February 2017

Global Sigfox Services Overview

External use under NDA

Table of content

Document Releases

Release *(Xyy)*	Date (*dd/mm/yy*)	Author	Modifications
1.0	10/02/2017	Sigfox	Document creation

1 Introduction

This document provides a general overview of the services provided by Sigfox and its operators to Channels (and its end-customers). Those services address all the activities of Channels dealing with the Sigfox technology from the pre-sales activities to the support of end-customers in the usage of the different services with a focus on the connectivity.

This document is organized around the following chapters:

- **Chapter 1: Introduction to Sigfox technology.**

  This chapter introduces the principles of the Sigfox technology in term of communication between the object and the network. It details the competitive advantages of this technology to address the IOT market.

- **Chapter 2: Sigfox network infrastructure.**

  This chapter describes the architecture of the Sigfox network with the different components, their roles & responsibilities. It explains as well the main workflows to provision devices, to process messages and to monitor the overall network. This chapter addresses as well transversal topics such as the security.

- **Chapter 3: End-customer services overview.**

  This chapter defines and describes the different services provided to the end-customers with in priority the connectivity service. It details the commitment in term of SLA from Sigfox and the Sigfox operators.

- **Chapter 4: Integration to the Sigfox ecosystem.**

  This chapter describes how Sigfox supports Channels to enter and to develop the Sigfox ecosystem with the portal dedicated to partners and the training program with certification to skill channel employees to the Sigfox Global offer. It details as well the pre-sales support with collaterals and demo kits.

- **Chapter 5: Sales tools overview.**

  This chapter describes the Connect Contracts platform that channels will use to do some quotations for end-customers and also to order subscriptions. It includes as well the different tools on the service coverage.

- **Chapter 6: Operations tools overview.**

  This chapter presents the Network & Operation platform allowing the service provisioning and all related services to manage activated objects. It includes as well the global support ticketing system and the reporting on SLA / KPIs on operations.

- **Chapter 7: Support processes.**

  This chapter describes the support process between end-customer, Channels, Sigfox Operators and Sigfox. It details the different levels of support and the workflows between them.

- **Chapter 8: Channel governance plan.**

  This chapter describes the operational organization between Channels and Sigfox Operators to support and to monitor the business.

Chapter 1

Introduction to Sigfox Technology

sigfox

2 Sigfox positioning

- **It's about connecting to the unconnected !**

Many of tomorrow's great ideas are technically possible today. They are just constrained by budget and energy issues. The reality is, small inexpensive objects simply don't have enough power to communicate with large mobile networks. That's 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 more importantly, enable a new range of opportunties for businesses across all industries. There are no limits to what can be acheived.

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, twoway, secured communication services to unlock the true potential of the Internet of Things.

Sigfox provides a standard way of collecting data from sensors and devices with a single, standards-based set of APIs. And 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 necessary to help companies and organizations make the most of their IoT ambitions.

3 Technology principles

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

3.1 Ultra-Narrow Band

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 bits per second.

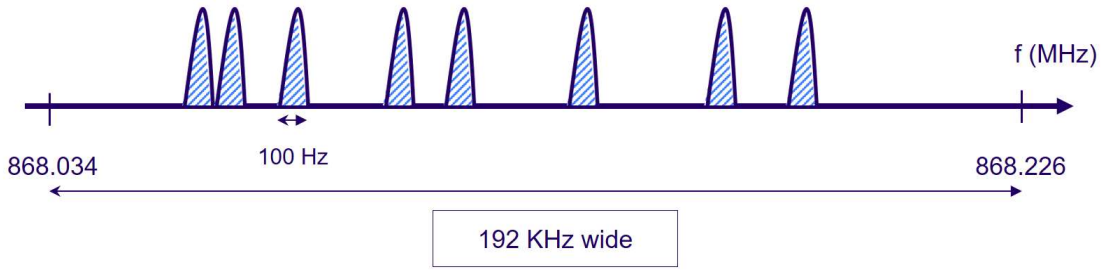


Figure 2: Sigfox technology based on Ultra-Narrow Band.

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

The band used is dependent on the location:

- In Europe, for example, the band used is between 868 and 868.2MHz.
- In the reste of the world, the band used is between 902 and 928MHz with restriction according to local regulations.

3.2 Random Access

The random access is a key feature to achieve high Quality of Service. The transmission is unsynchronized between the network and the device. The device broadcasts a message on a random frequency and then sends 2 replicas on different frequencies, which is called “frequency hopping”.

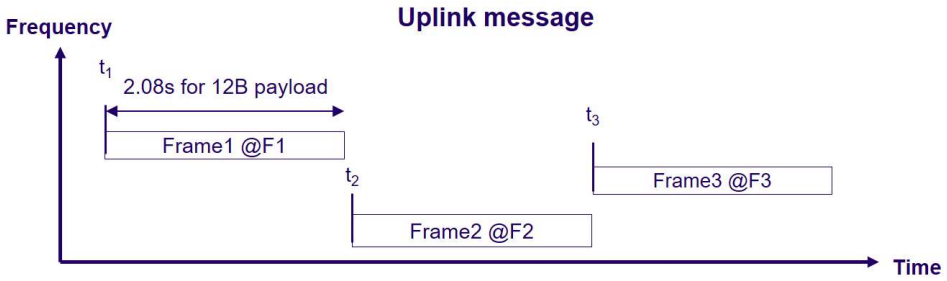


Figure 3: Frequency hopping on replicas.

A message with a 12-byte payload takes 2.08s over the air.

The Sigfox Base Stations monitor the 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 broadcasted message is received by any base stations that are nearby and on average the number of base stations is 3.

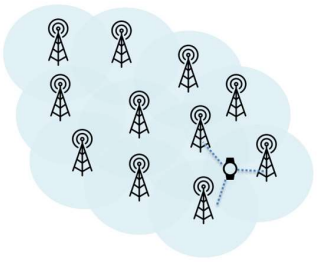


Figure 4: Message reception by multiple Sigfox Base Stations

The spatial diversity coupled with the time and frequency diversity of the repetitions are the factors explaining 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 take 6 bytes
- A temperature 2 bytes
- Speed reporting 1 byte
- An object status 1 byte as well
- A “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 for the moment.

For downlink messages, the size of the payload is static: 8 bytes. Again on 8 bytes, a lot of information can be transferred. It’s 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's 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 delta.

4 Key features of the network

This chapter addresses the main characteristics of the Sigfox network itself in term of architecture & performances.

4.1 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 had been used but a software algorithm instead to handle demodulation in an effective manner. It reduces significantly the TCO.

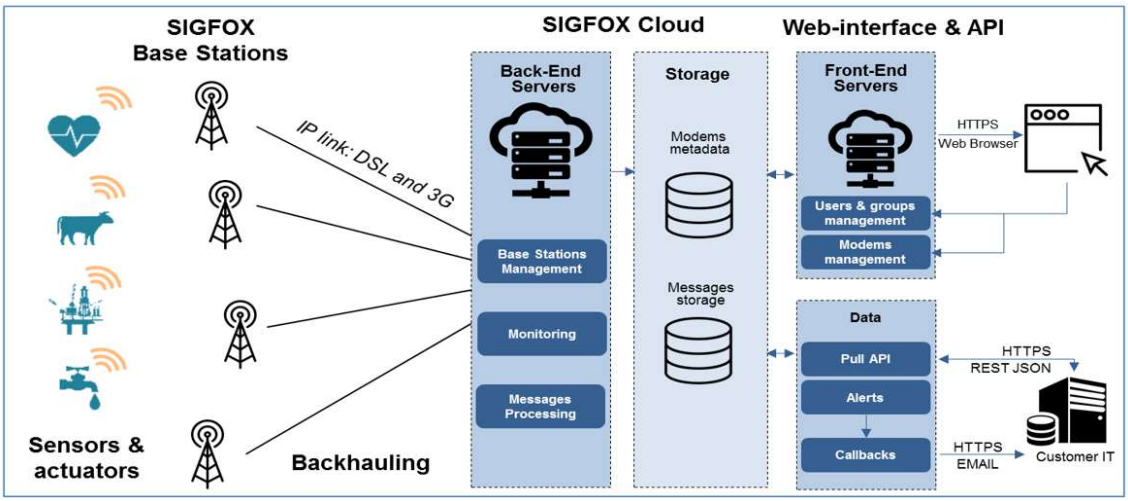


Figure 5: Flat architecture

The data is sent over the air to the base stations, then goes through the backhaul. The backhaul uses DSL connectivity mostly 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 on one side to be used for building services and the customers' messages on the other side so that customers can retrieve them later.

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

4.2 High Network Capacity

The capacity of the network is high, enabling Sigfox to scale for the billions of objects. The massive capacity of the Sigfox network infrastructure 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 signal.
- The frequency and time diversity introduced by the random access
- The spatial diversity due to the overlapping network cells

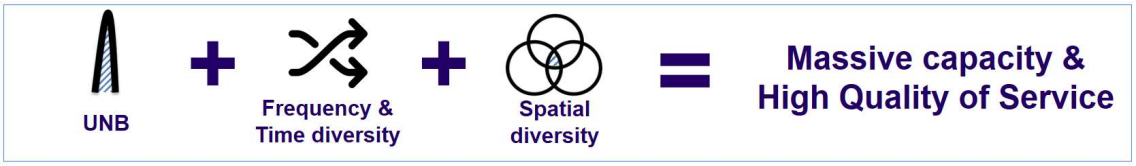


Figure 6: Combination of Sigfox specificities

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

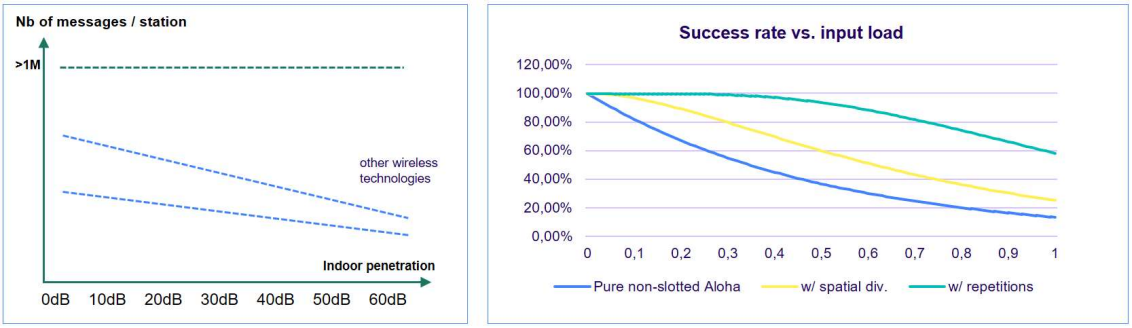


Figure 7: Capacity sustaining whatever the quality of the radio link

If the targeted Quality of Service is 99,99%, The load on the base station shall not be higher than 14%. In other words, from around 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%.

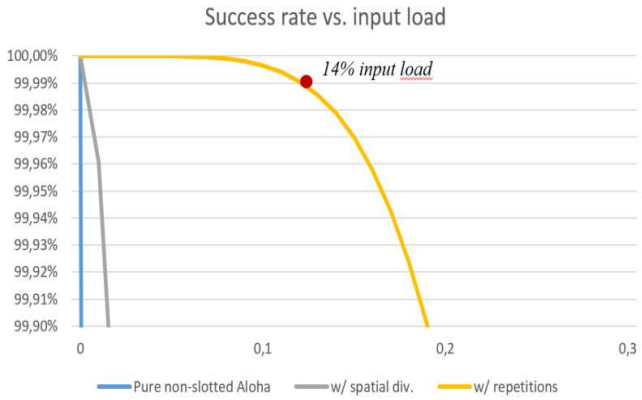


Figure 8: Limited impacts of the load on the Quality of Service thanks to repititions

4.3 High Energy Efficiency

The high energy efficiency enabled by Sigfox technology relies also 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 true 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 6 times inferior therefore the battery life is about the same.

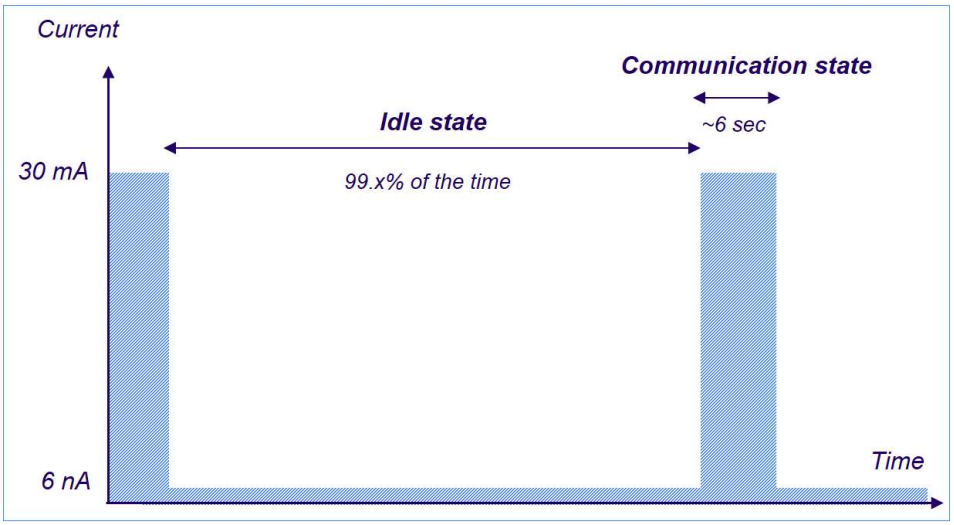


Figure 9: Low idle consumption increasing the battery life

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

- No pairing is required meaning that there is no synchronization message exchanged between the object and the base station before transmitting the data. This is a big advantage vs. other technologies which all have this additional step.
- Also the idle consumption is very low, often a few nano Ampere making it almost negligible.

4.4 Long Range

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

- For a given output power, the range of the RF link is determined by the data rate, i.e. lower rate provides 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.

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.

When talking about 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 2.4GHz, will suffer for indoor use cases.

4.5 Resilience to Interferers

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

For the same technical reasons as above, UNB is extremely robust in an environment with other 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 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 8dB above the noise floor.

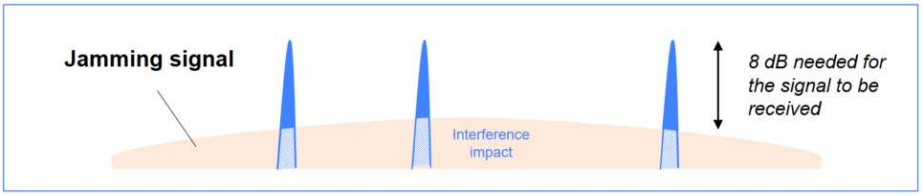


Figure 10: Resilience to interferers providing by UNB

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.

4.6 Security by-default

The Sigfox ecosystem integrates the security by-default:

- Authentication + integrity + anti-replay on messages propagated on the network.
- Cryptography based on AES with no key transmission by OTA.
- 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 3 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: 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's ID has not been duplicated. In the case of a corrupted device, there is a blacklist list mechanism to 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.

Chapter 2
Sigfox Network Infrastructure

sigfox

5 Sigfox network architecture overview

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

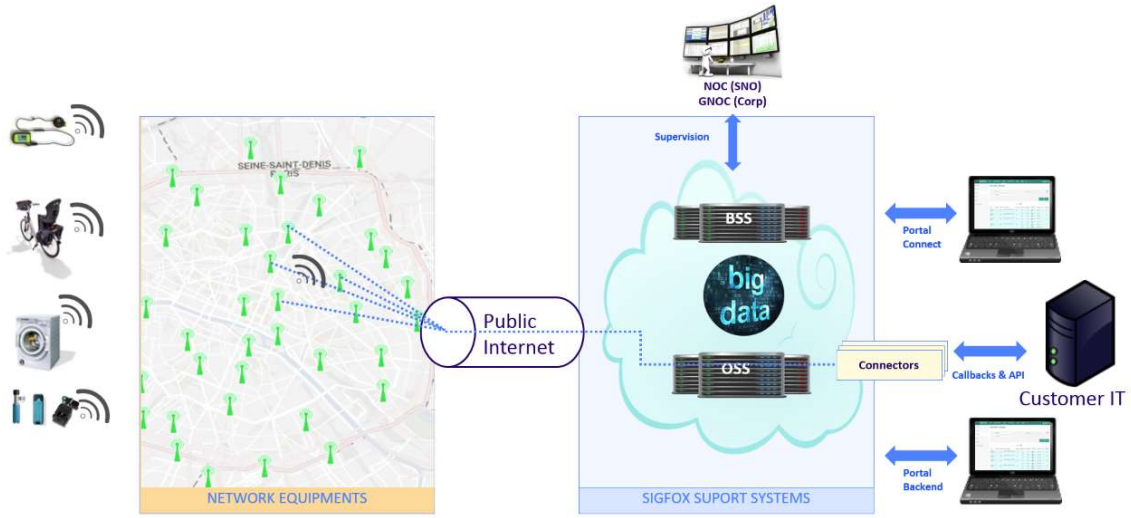


Figure 11: High level architecture of the Sigfox network

The Sigfox network has a horizontal & thin architecture composed of 2 main layers:

- **The Network Equipment** layer constitutes 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 to 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 & end-customers) to interact with the system through web care interfaces or APIs. This layer includes as well modules & features key 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. This layer includes as well repository and tools to analyze data collected or generated by the network.

As mentioned in the figure above, the link between the 2 layers is ensured by the public internet but secured with VPN connection.

The following chapters describe the different components of those 2 layers of the Sigfox network.

6 Network equipment

The Network Equipment layer includes the different elements of the network responsible to receive messages from devices to transmit them to the Sigfox Support System.

The Network Equipment layer is composed of the following components:

- The Base Stations

  They are in charge of receiving messages from devices, checking its integrity (against interferences) and transmitting it to the Sigfox Support System through a data connection protected by a VPN. There are several types of Base Stations in the Sigfox Network with various capabilities in term of coverage, traffic to handle.

  The Sigfox Base Stations are a multiband compact base stations suitable for primary coverage and densification. They may be installed in very divers environments from busy city to rural environments away from cellular or broadcast sites.

  The standard installation includes the Sigfox Base Station, a low noise amplifier (LNA) that can be combined with a cavity filter (LNAC), an antenna and connections to the internet.

Figure 12: Main components of a Sigfox Base Station

  There are 2 types of the Sigfox Base Stations:

  - The Macro Base Stations in charge of covering a large area with as well capability to support huge traffic with hundreds of devices. They are able to cover outdoor locations as well as a part of indoor locations.
  - The Mini Base Stations in charge of covering a small area with a limited number of devices can address locations not covered by the Macro Base Stations such as rural area or indoor locations.

- The Repeaters (available in Q3 – 2017)

  In the coming months, the Network Equipment layer will be enriched by repeaters that are different from base stations: Repeaters are able to repeat messages coming from a device to a base station. This component will enable locally the extension of the coverage for a limited number of devices.

The combination of the different base stations & repeaters aims at ensuring the maximum coverage on the field and at answering to specific deployment cases.

The following paragraphs described those different components as well as the general strategy to deploy efficiently those different components.

6.1 Macro base stations

Sigfox Macro Base Stations are ultra-wide range, high linearity transceivers and feature first class performance radio and innovative software defined processing, for use in Ultra Narrow Band IoT wireless communication systems. The key features are:

- Long Range Radio transmitter.
- Software Defined Radio operation.
- Ultra low receiver sensitivity.
- 120dB receiver linearity.
- Web based management tools.

Figure 13: Macro Base Station SBS-T-v2.2 and SBS-T3 (Access Station)

The latest version, the SBS-T3 Base Station, called Access Station, is the industry's highest capacity macro base station enabling massive IoT wireless communication solutions.

The product is based on the carrier grade SBS-T Base Station platform with low power consumption and high level of integration, comprising radio, baseband and backhaul functionalities with Ethernet & Cellular connectivity. The base station can receive and transmit millions of messages per day.

SBS-T3 is compatible for operations in SRD and ISM bands across the World, compliant with ETSI, FCC, ARIB and many more standards. With compact form factor and IP65 rating, SBS-T3 is suitable for both outdoor and indoor installations.

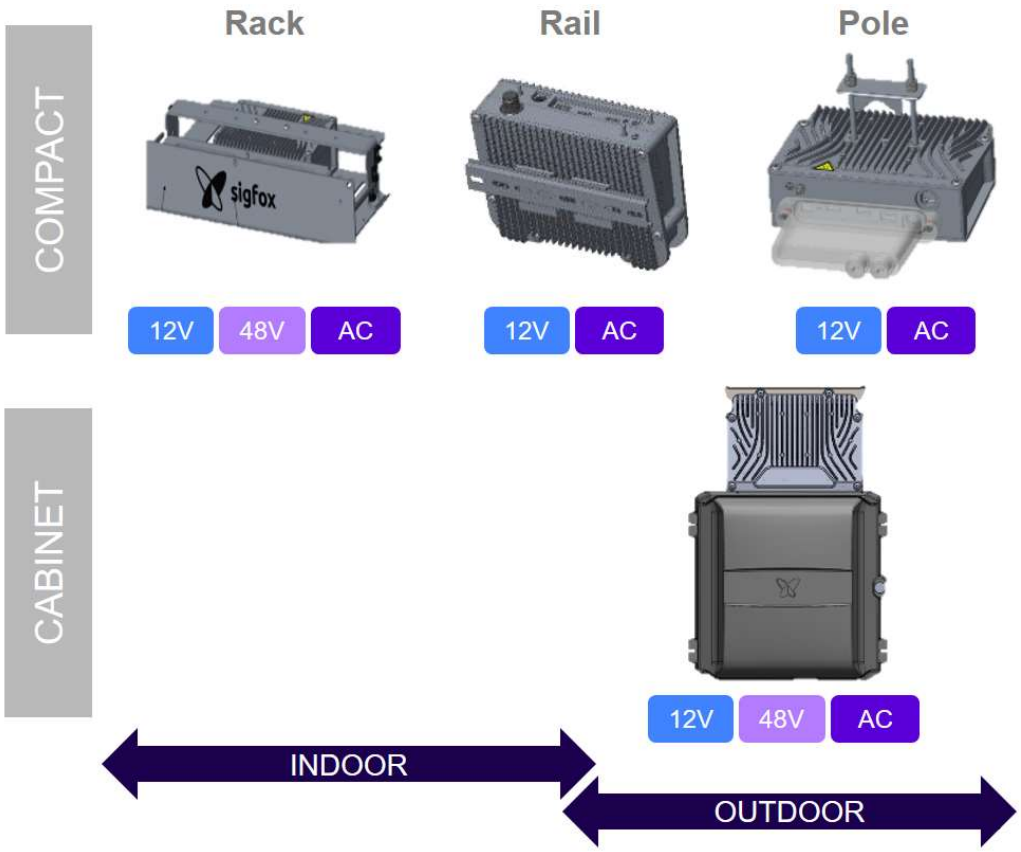


Figure 14: Different installations & mounting types of the SBS-T3 (Access Station)

Improvement has been made to reduce its size and weight, increasing its robustness and keeping the same performances.

The Base Stations are available in two frequency variants targeting worldwide IoT applications:

- The 865-870 MHz band.
- The 902-928 MHz band.

6.2 Mini base stations

Sigfox SMBS-T is a multiband compact base station suitable for coverage extension complementary to the Macro Base Stations.

Figure 15: Mini Base Station SMBS-T

SMBS-T is specifically dedicated for indoor coverage densification hence a perfect solution for IoT custom projects to complement primary macro coverage layer. It may also be installed in rural environments away from cellular or broadcast sites.

SMBS-T is compatible for operations in SRD and ISM bands across the World, compliant with ETSI, FCC, ARIB and many more standards.

With compact form factor and IP65 rating, SMBS-T is suitable for both outdoor and indoor installations, especially: mast mounting, wall mounting, and desktop installation.

These series are dedicated for quiet radio environments with limited performance for capacity and blocking resistance. This gives a complementary solution for the Sigfox network based on Macro Base Stations.

Regarding capacity performances, the SMBS-T is able to receive about 100 000 messages per day.

The installation site, and in particular the antenna elevation, shall be chosen so that the number of Sigfox devices covered by the SMBS-T antenna is compliant with this capacity.

6.3 Repeaters (available in Q3-17)

The repeaters will be a new type of Network Equipment ensuring locally the extension of the network coverage for a limited number of devices.

The repeater will repeat messages coming from devices around to Base Stations. It will support only the uplink messages from devices to the Sigfox Support Systems. Downlink messages will not be supported. Devices will have to be up to 100s meters around the repeater to be supported. This means that the repeaters will be used to extend the coverage at its edge for limited areas and in specific case such as deep underground, building, warehouse, …

The repeater will integrate a white list mechanism filtering devices relayed: Only devices included in this white list (by using their IDs) will have their messages repeated by the repeater. The other will be ignored. The repeater will be able as well to repeat all messages received whatever the device if the white list mechanism is disabled.

The repeater will be able to support only 10s of devices.

The repeater will be easy to install anywhere without any backhauling requirements as it will be autonomous in term of energy with a battery that will have a life duration up to 5 years.

The equipment should have different form factors depending on the use case. The following picture is an example of form factor:

Figure 16: Example of repeater form factor (source: Adeunis)

The repeater will not be produced and provided by Sigfox. It can be provided by a Sigfox Operator or designed specifically for an end-customer according to its usage and constraints.

The deployment of this repeater will be ensured as well more by the end-customer.

6.4 Deployment strategy

Macro & Mini Base Stations and repeaters aim at providing the optimized service coverage to the devices. The following scheme details the different types of coverage and which network equipment will be in charge to support it:

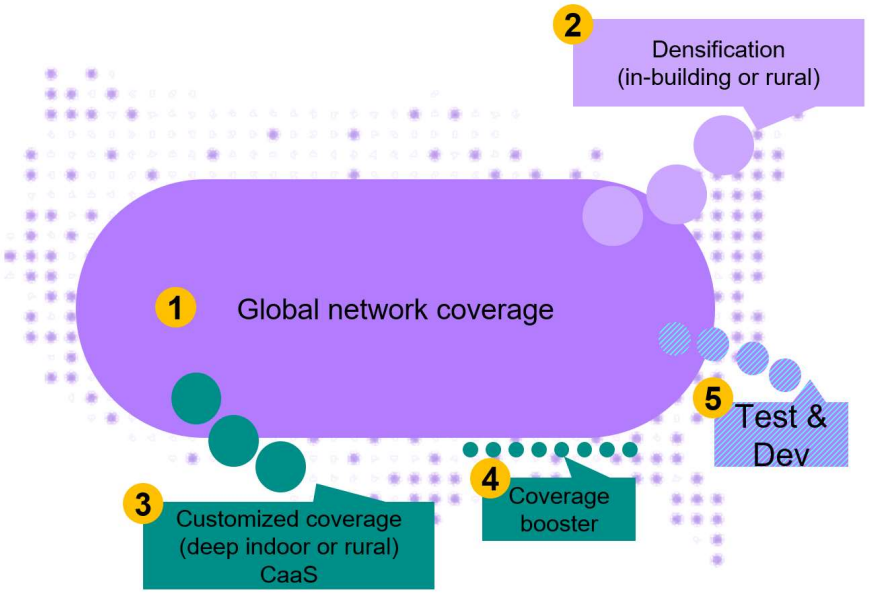


Figure 17: Different coverage layers

- The Global network coverage is the primary layer that aims at optimizing the coverage in term of area and population for outdoor and also to address indoor. This coverage is ensured mainly by the Macro Base Station.
- The densification aims at extending the coverage mainly for indoor with building and also for rural locations not covered by the primary layer. Macro and Mini Base Stations can be used for this densification.
- The customized coverage aims at supporting locations for a specific customer who has locations not supported by the 2 previous one. In that case, the customer will lease a base station to cover this area using the "*Coverage as a Service*" offer. This offer is generally based on Mini Base Stations.
- The coverage booster aims at locally extend the coverage for few devices in case of deep indoor use cases generally. This is ensured by the repeater.
- The Test & development coverage aims at providing to device makers or start-up means to develop and to test devices integrated the Sigfox technology whereas they are not covered. Mini Base Stations are essentially used with a "*Coverage as a Service*" approach.

7 Sigfox Support System

The Sigfox Support System constitutes the core infrastructure of the Sigfox network with the following functional architecture:

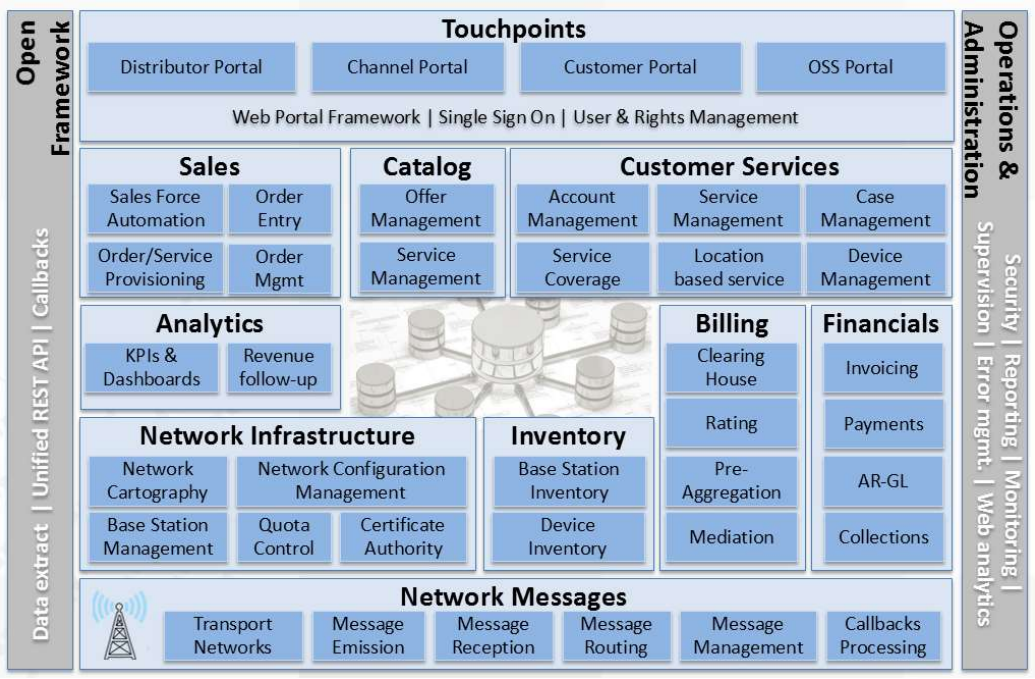


Figure 18: The functional architecture of the Sigfox Support System

- **Touchpoints layer:** This layer corresponds to the different web care interfaces provided on top of the Sigfox Support System addressing different types of users.
- **Customer services:** This is a set of services used by Sigfox Operators or customers.
  - Service coverage: This module is responsible on one side to provide maps indicating the service coverage with the associated quality of service and on the other side API providing the service coverage on locations given by the customer.
  - Device management: It handles the activation process of devices.
  - Account, Service & Case management: They aim at managing the relationship with customers such as support with ticketing tool.
  - Location base service: It is a service providing location information on devices based information collected at the network.
- Sales modules:
  - Order entry: It allows creating quotation and proceeding it to an order.
  - Order management: It tracks and manages orders by also distributing it to the different applications. It sends the order to the appropriate applications and manage the workflow execution. It provides a status. The definition of

the workflow is ensured by the Order & Service provisioning function defined below.

- Order & service provisioning: This function aims at defining the order fulfillment with the workflows to execute in case of orders on the different offers and services. It also details the main characteristics of the offers & services.
- Sales force automation (not yet available): This function manages the sale life cycle with business objectives, forecast & performances, opportunity follow-up, tracking of customer interactions, …

- The service catalog:
  - Offer management: This is the unique repository of product & service offering that includes rules of product fulfillment (delivery), compatibilities, pricing and availability. The fulfillment rules are used for the ordering management to define the execution plan. The pricing rules are used for the quotation and the billing to compute fees.
- Billing components:
  - Mediation & pre-aggregation: Those modules aim at retrieving, formatting and aggregating data from the network detailing the usage of the different services by devices.
  - Rating: It computes based on the information coming from the pre-aggregation module and as well the pricing of the services the different elements of the invoice for a customer.
  - Clearing House: In the case of Sigfox having a global approach sustained by different local operators, the Clearing House is responsible of the clearing & settlement between the different Sigfox Operators. It prevents complex billing & financial flows between operators.
- **Financials modules:** Those modules are in charge of the invoicing & payment of the Sigfox Operators based on the computation done by the Rating & Clearing House modules.
- **Analytics tools:** They are aggregating information coming from the network on usage but as well from billing modules in order to monitor and report globally KPIs on the network and also revenues generated.
- Network infrastructure:
  - Network cartography & radio planning: They allow simulating and evaluating the network coverage in order to position new base stations to install for example. The results are also used to create maps providing the service coverage.
  - Base station management: This module allows managing base stations, their life cycle, the maintenance operations to execute, the upgrade of the software installed on it, …

    - Network configuration management & quota control: They manage the different parameters on the network in term of configuration of the base stations, usage of the services, …
    - Certificate authority: This module manages the different security assets to enable devices to access to the network, base stations to communicate to the core network, …
- **Inventory:** It manages & stores information on base stations and devices that is used for the device management or for the remote management of Network Equipment.
- **Network messages:** It constitutes the core network of the Sigfox Support Service managing the processing of messages coming from devices through base stations.
    - Transport networks: It is responsible of the communication between base stations and the infrastructure by managing a secured connection based on VPN.
    - Message reception, emission & routing: They are responsible respectively to receive uplink messages and to send downlink messages to the right base station.
    - Message management: It takes care globally of the management of the different messages thanks to the level of subscriptions provided to the device.
    - Callback processing: It is responsible to send the received messages to the customer IT system.

The following paragraphs provide more details on the key components of the Sigfox Support Service by segmenting it between:

- **Operation Support System** that is the combination of the functional modules included in “Network Infrastructure”, “Network Messages” & “Inventory” described above, is responsible mainly of the message processing to the callback generation and the management of the Network Equipment.
- **Business Support System** combining functional modules from “Sales”, “Catalog” and “Billing” enables the management of the different services provided and the business processes to quote, to order and to bill services.
- **Core Network Monitoring & Performance** that provides a secure, reliable and scalable infrastructure for the Sigfox Network, Backhaul and OSS (VPN, callbacks, data center inter-connexions) and monitoring metrics aggregation for Base Station and monitoring platform (NIP/NOC and GNOC).

7.1 Operation Support System

The Operation Support System (OSS) is composed of the following technical components:

- **Receiver**: The core business component that processes all messages received by the base stations and reacts depending of the configuration made by customer in the web portal (deduplication, callback, mail, reject msg, bidirectionnal...)
- **CRA (Central Registration Authority)**: The global component in charge of the device & base station ID's generation. It is also in charge of the generation of the device private communication keys in order to sign every radio messages for authentication.
- **Callback module:** It is in charge of the processing of the callbacks to the customer IT system at the end of the message processing chain in the receiver. It is as well the entry point for the bidirectional communication with the devices by providing the downlink messages to be sent to the devices.
- **Management modules on base stations and devices:** They are respectively responsible of the remote management of the base stations and device provisioning.
- **Radio planning:** This tool allows to simulate & evaluate the network coverage thanks to the base station locations and geographical (and social) information on territories.
- **Web portal**: Main interface for SO & customers. A Web portal which allows to configure devices, callbacks, base stations, launch radio planning simulations and so on ...

7.1.1 Receiver

The receiver has the following functionalities:

- Message collecting: It receives messages from all base stations deployed in the different territories.
- Command manager: It executes predefined command at reception such as response, email, callback, ... This is a kind of workflow engine.
- Message processing: It de-duplicates messages and send them to customer IT infrastructure through the callback module.

The following paragraphs detail mechanisms and processes involved in the message processing.

7.1.1.1 Principles of the message processing

Each radio message is sent three times and can be received by several base stations (3 in average). In average, a given actual device message is composed of 9 individual messages (3 repetitions x 3 base stations).

These individual messages are de-duplicated in order to send a unique and useful message to the customer's IT system. The first processed repetition of a device message is the one which triggers the callback to the customer's IT system. The other repetitions of the message are just metadata to complete the message information.

A priority queue is used to determine the message processing order:

- **HIGH**: uplink messages asking for downlink responses (in time and without over usage -> max 4 downlink messages per day)
- **MEDIUM**: first repetition of a standard uplink message (in time)
- **LOW**: everything else (other repetitions of the messages, late messages, BIDIR over usage, etc...)

7.1.1.2 Message payload display types

It can be defined at the device type level:

- **None**: Raw data.
- **Custom**: Use a custom grammar to display a user friendly information of the message payload.
- **Geolocation**: Display the location of the GPS device from GPS formats known by the system.
- **String**: Display the payload as an ASCII text
- **SensitV2**: Display Sensit V2 payload format in a user friendly way.

7.1.1.3 Message grouping

In order to limit network load, the base stations group messages by “batching” the requests to the cloud with a limit of 100 messages per request.

7.1.1.4 Message checks

There are the following message checks executed for uplink messages:

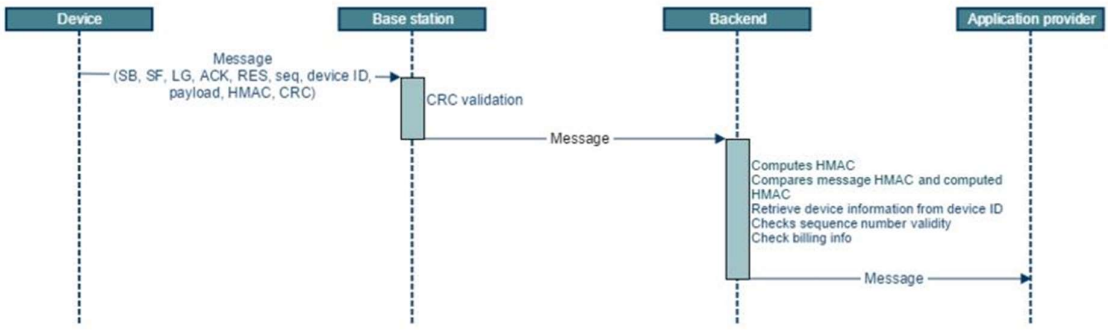


Figure 19: The different checks executed along the uplink message treatment

Note: More details on the different checks are provided in the section dedicated to the security.

7.1.1.5 Out Of Band messages

Out Of Band (OOB) messages are network messages without user data payload. There are 3 types of OOB messages:

- Downlink Acknowledge: This message is generated by a base station during the downlink process in order to give back a status of the procedure (if everything goes well or not).
- Keep Alive payload: This message is generated by the device to give some technical information regarding the device itself such as the temperature and the power tension, etc...
- Rollover synchronization counter (used for the sequence number): This message is generated by the device to help resynchronizing the rollover counter of this device in the cloud database. The rollover counter is used to decrypt encrypted messages.

7.1.2 CRA

- The CRA is the Central Registration Authority. It is a global entity in charge of the device & base station ID's generation. It is an essential component for the device and base station manufacturing. It is also in charge of the generation of the device private communication keys in order to sign every radio messages for authentication.
- Device credential generation

Each device needs to have a unique ID in the Sigfox global network. The CRA is the entity in charge of generating these device IDs and also their NAK (Network Access Key) and their PAC (Porting Access Code).

Hardware manufacturers producing Sigfox devices are provided with ID range to produce along with their NAK. A pair of ID/NAK is flashed into each manufactured device firmware.

NAK is a private communication key per device that is used to sign every messages for authentication.

PAC is a required code to provision a device in the system and to change operator and/or customer. It is a one-time code. A new one is generated after each use. A customer can change operator or sell its device to another customer. In that case, he needs the PAC to activate the transfer of the device. However the most common use case is that the final customer never connect to OSS Web Portal but only to partner backend portal if any.

- Device / operator association

The CRA knows anytime at which operator a device belongs to. It is the reference inventory of all manufactured devices and base stations. It is essential for a global network approach and especially for the roaming function.

7.1.3 Callback module

When a message needs to be acknowledged, the callback selected for the downlink data must send data in the response. It must contain the 8 byte data that will be sent to the device asking for acknowledgment.

There are two types of downlink modes:

- **Direct**: When a downlink request is received from a device, the data configured in the "Downlink data in hexa" field is provided as a payload for the downlink message.
- **Callback**: When a downlink request is received from a device, the configured downlink callback will be pushed by the Sigfox Support System to the partner's IT platform. Then, the IT platform may provide the downlink payload to be transmitted by the network to the device. If this feature is used one must also create and enable a downlink callback in "Device type > Callbacks".

The OSS Portal can automatically forward some events using the «callback» system. The configuration of callbacks is done in the device type page.

The callbacks are triggered when a new device message is received or when a device communication loss has been detected. When receiving a callback, the client system must return an HTTP 2xx code within 10 seconds. If the client system fails to process the callback during this time, an automatic retry will be scheduled 1 minute later.

The customer can create callbacks of 3 different types with different set of available variables for each type of callback. These variables are replaced by their value when a callback is called:

- **DATA**: A “Classic” callback containing user payload (12 bytes) and some metadata (timestamp, sequence number, ...).
- **SERVICE**: A callback to receive the status of the device (battery voltage, temperature, ...).
- **ERROR**: A callback to notify device communication loss. If a device is supposed to communicate at least every x mins and it doesn't, this callback is triggered.

Only DATA callbacks provide user payload to the customer. A downlink message can be given by the customer's IT in response of a DATA callback (limited to 4 messages per day in Sigfox contract).

Then the callback medium defines the way to forward the event. The two mains functions are:

- Email.
- HTTP (simple and batch).

For HTTP simple callback, each message is directly forwarded in a single HTTP request. “HTTP GET”, “POST” or “PUT” method can be used, although POST method is recommended.

For the batch method, messages are gathered together per callbacks, each line representing a message, then sent in batch using a single HTTP request every second. This avoids a possible peak load that the customer server can possibly not handle. As the payload contains multiple messages, only HTTP POST method are supported.

- **Downlink** callbacks

When a message needs to be acknowledged, the callback selected for the downlink data must send data in the response. It must contain the 8 byte data that will be sent to the device asking for acknowledgment.

7.1.4 Radio Planning

The Radio Planning is a built-in tool provided in the Sigfox Support System to simulate and to evaluate the network coverage on territories:

- Simulation to create the coverage on a new territory or to extend of an existing network to address new locations or densified existing one.
- Evaluation to provide the service coverage on the different territories to the Sigfox eco-system and to customers. This evaluation can be checked and fine-tune with field tests.

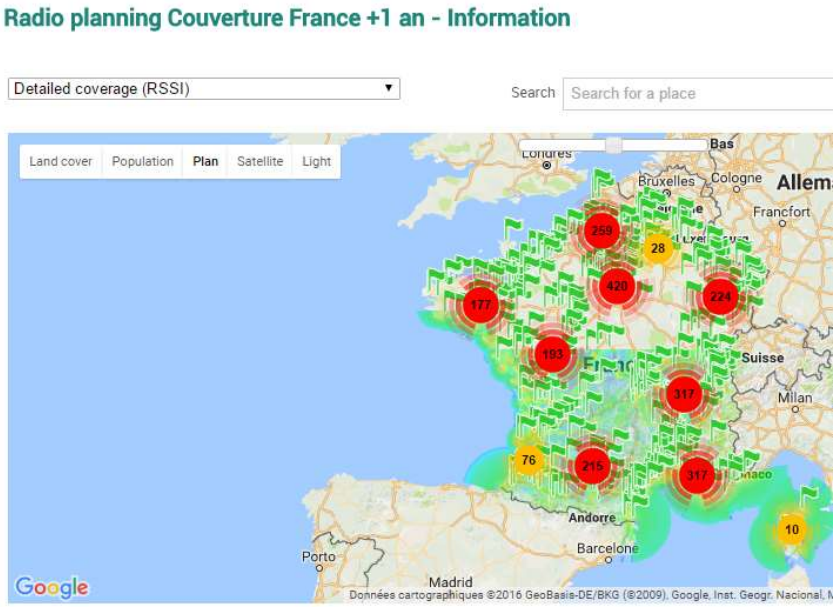


Figure 20: Radio planning to simulate & evaluate the network coverage.

In addition to the simulation & the evaluation, the Radio Planning will provide the information needed to generated the different maps displayed in Sigfox solutions:

- Coverage maps (with various settings & render mode).
- Target fulfillment maps.
- Landcover maps.
- Population density maps.
- gmaps tiles.

There are public maps (as for the public Sigfox website), shared maps integrated to the Sigfox Support System such as the global public coverage and private maps for Sigfox Operators which could simulate antenna deployment effect in simulation.

For coverage maps, there are various displays available:

- Simple coverage.
- Detailed coverage RSSI.
- Detailed coverage margin.

- Service overlap with different margins & class.

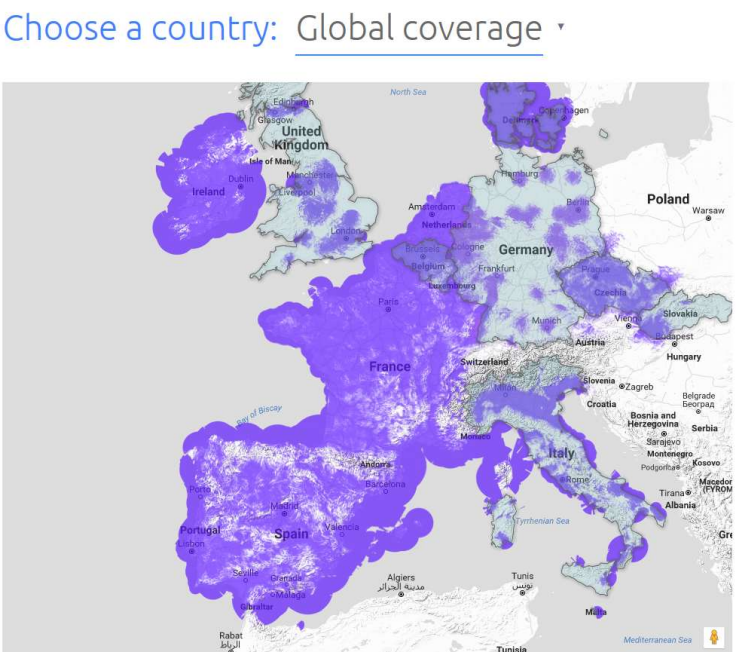


Figure 21: Radio Planning results used to generate coverage maps.

Note: RSSI stands for Received Signal Strength Indication, it is a value in dBm which represents the level of signal at the base station antenna. Using the max link budget (or MaxDb) and environment loss for each station, a margin value in dB is calculated according to the following formula: Margin = (RSSI - MaxDb - EnvLoss).

Additionally, the global coverage could be seen for actual situation or for a forecast situation.

7.1.4.1 Overview on the simulation process

The simulation process with the Radio Planning tool is executed in X steps:

1. Creation of a new simulation project

The Sigfox Operator is able to create a new project with some functionalities such as being the clone of a territory already in production or being a forecast project that will display all statistics. The “clone” project is used to simulate the extension of the coverage with the integration of new base stations.

This is also possible to define if the simulation will be visible on the coverage map.

2. Importation of new sites

This step aims at importing in the Radio Planning tool one or several sites in the simulation. Those sites will complete the existing ones in the case of a clone.

This importation can be done manually by providing detailed information on this new site such as the latitude, the longitude, the height above the ground and other characteristics on the ecosystem influencing the propagation.

This importation can be done by batch with a CSV file including the main information mentioned before on the site. Once the upload of the file is done, there is a report provided by the Radio Planning tool to mention the number of sites imported and the potential issues during this operation.

3. Simulation running

Once all sites had been imported in the project, the simulation can be launched. A progress bar indicates the progress on the execution.

4. Simulation view

Once the simulation is finished, it is possible to visualize the results with different views:

- Simple coverage
- Detailed coverage (RSSI or Margin).
- Max Link budget (up to -142 dBm).
- Link Budget with 20 dB margin (Indoor daylight: up to -122 dBm).
- Link Budget with 30 dB margin (Deep indoor: up to -112 dBm).

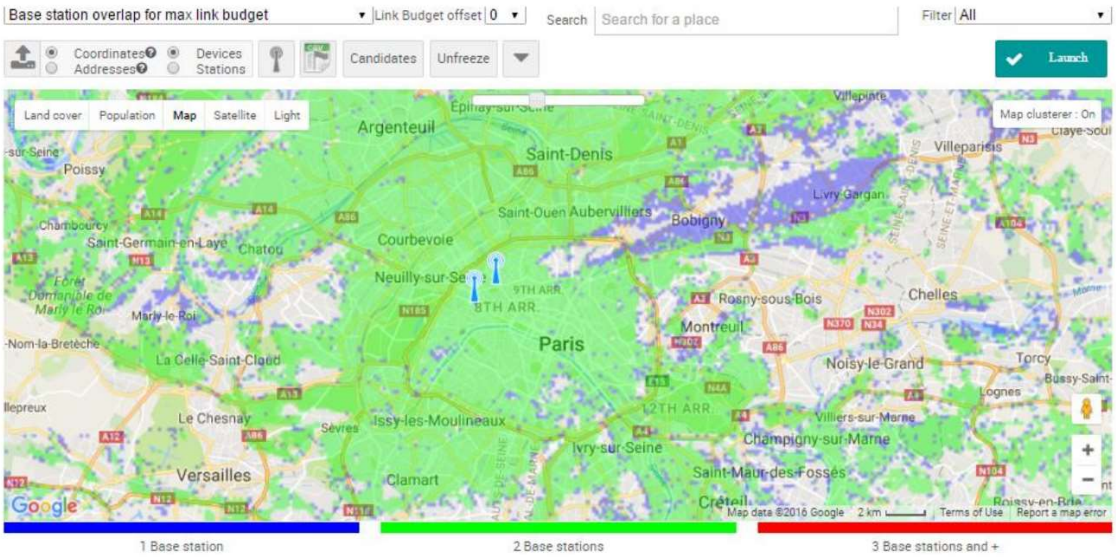


Figure 22: View of the simulation (base station station overlap for Max Link Budget)

Several layer views are available on the map such as the population density, land cover layer, satellite view & relief view in order to evaluate the impacts of the simulated coverage on the population for example:

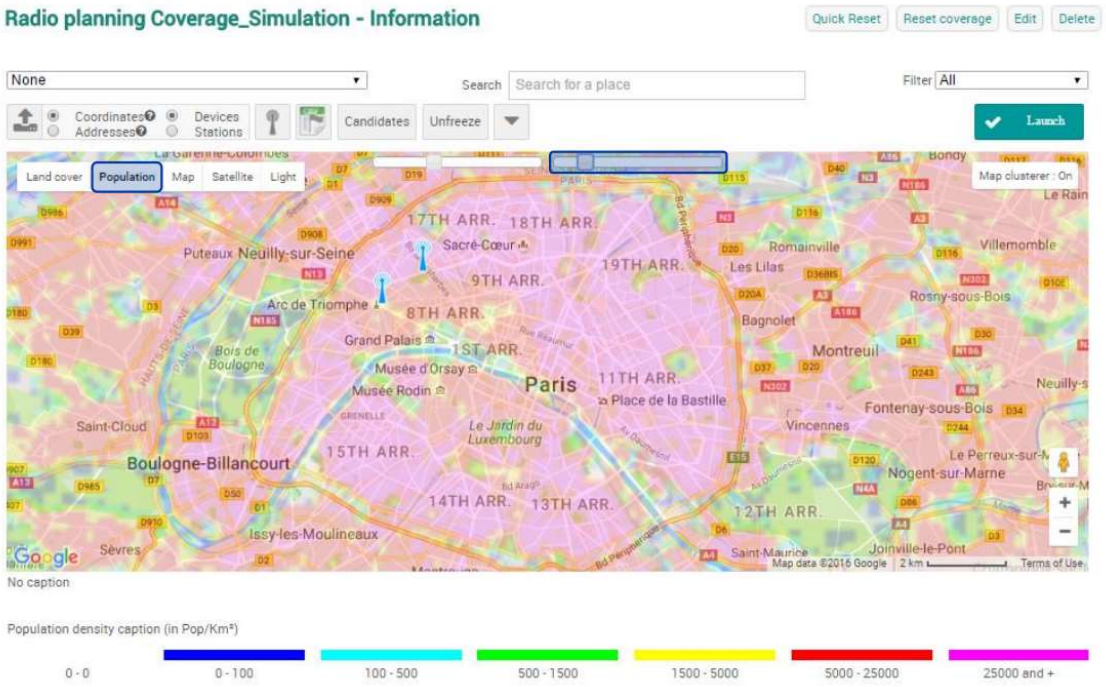


Figure 23: Additional layers to maps to compare simulation results with other factors such a population density

7.1.4.2 Calculation

Coverage maps calculation are all based from Sigfox Base Station RSSI accumulation with various simple transformation. All real, forecast or simulated Sigfox Base Station RSSI coverage is calculated once by the Radio Planning software.

Then the portal sub-divides result on an Universal Transverse Mercator like grid (tile from 1 degree by 1 degree called MapUnit or Graticule) individually and stored in a collection indexed by latitude & longitude for all Sigfox Base Station individually.

Signal aggregation is calculated all in Java portal code and result are stored in cache (mongo). Signal aggregation is a summing operation: Aggregate two stations is simply adding there RSSI point by point (same for margin).

Main aggregation data are (pixel per pixel):

- Cumulated RSSI.
- Max margin of all BS covering this pixel.
- 2nd max margin of all BS covering this pixel.
- 3rd max margin of all BS covering this pixel.

7.1.4.3 Cache management

When a Sigfox Base Station is added, the Radio Planning software simply adds the corresponding Base Station RSSI to previous aggregated tiles and eventually change the 1st/2nd/3rd max margin if needed.

More frequently used data aggregation visualization are persisted. These results are stored in png format.

On the other hand, when a base station is deleted (or updated) all previous aggregation MapUnit of the area is invalidated and need to be recalculated.

There is no need to relaunch the Radio Planning software on all Base Stations (Base Station individual results are stored in mongo).

7.1.5 Web Portal

The web portal provides an access to the following features of the Operation Support System:

- Base station & site management with main information and maintenance operations.
- Radio Planning to simulate & to evaluate the network coverage.
- Station management to remotely manage the base station and its embedded software.
- Device Management.
- Access to messages generated by devices.
- Diagnostic.
- Alerts Batches.
- Billing / Contract.
- Billing Batches.
- Statistics.
- Single Covered TAP.
- User/Group Management.

On user administration pages, there is a “Go” button which allow admin to see the portal “as it is” for this user. This capability is very useful to check authorizations.

7.2 Business support system

7.2.1 Product catalog

The connectivity subscription is made simple with customizable Retail Price Grids.

Sigfox’s geolocation service (*Spot’it*) can be activated when making an order.

7.2.2 Quote & order management with Connect Portal

The Sigfox Connect portal is part of the Business Support Solution (BSS) to help manage Sigfox subscription contracts and monetize IoT solutions.

The Scope of Sigfox Connect Contracts goes from quote simulation to order creation:

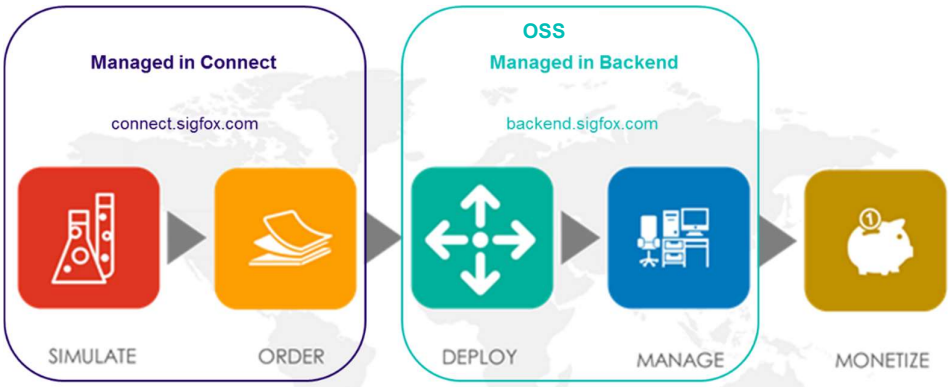


Figure 24: Scope of Sigfox connect

The main functions of Sigfox connect contracts are the following:

- Register Distributors and Channels (CPA or Prospect)
- Simulate quotation over a large number of countries
- Validate an order
- Create Customer group
- Group/User management

7.2.3 Billing

7.2.3.1 Roles

Sigfox provides billing service to its distributor in order to provide all data needed for them to invoice their channels.

Figure 25: Billing process overview

As described below, Sigfox billing process is composed of 4 steps going from usage data aggregation to invoice generation. This implies actions from Sigfox and its distributor.

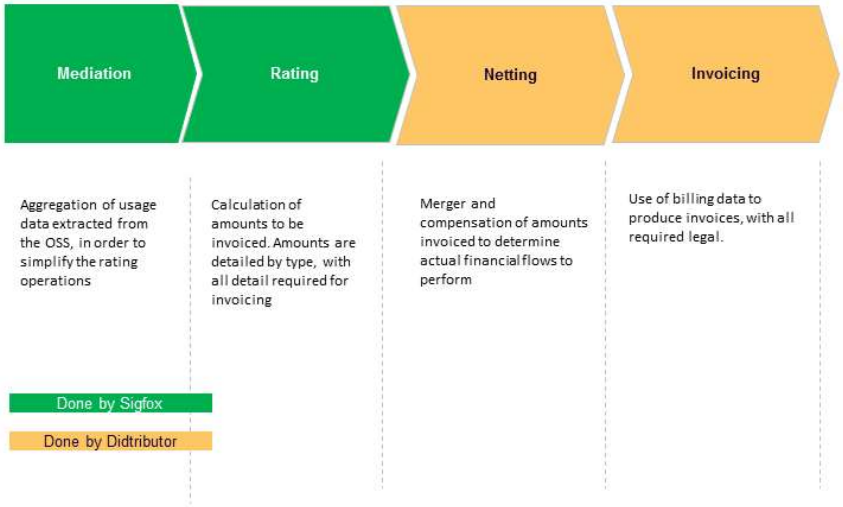


Figure 26: Different processes around the billing

Sigfox billing is based on monthly bills and monthly invoices.

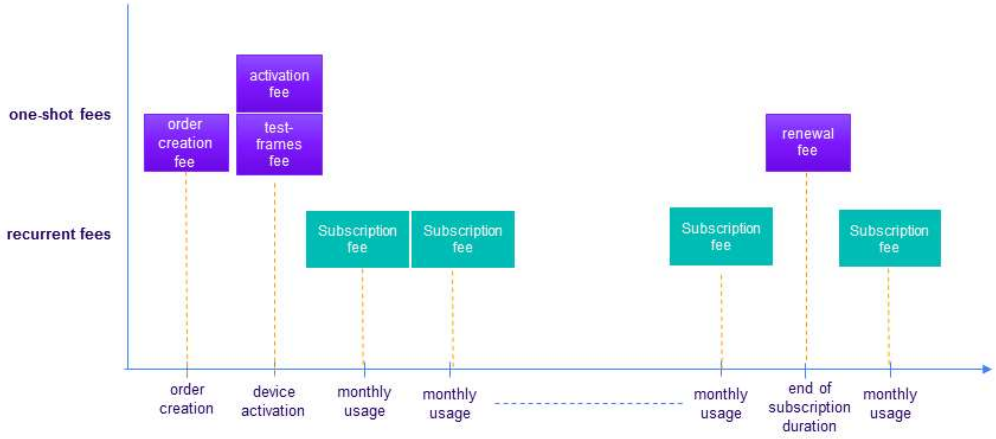


Figure 27: Fees billing chronogram

7.2.3.2 Data format

The distributor provides detailed data in CSV format to channels. There are two kinds of files:

- A summary that summarize per channel the amount to pay for all fees.
- Per fee detailed files that shows per order the usage data needed to calculate the concerned fee:

- Order creation fees details: Billing month, order description fields, number of device allocation per territory and related order creation fee amount.
- Activation fees details: Billing month, order description fields, number of device activations, related activation and test-frame fee amount.
- Subscription fees details: Billing month, order description fields, number of billable days and related subscription fee amount.

Renewal fees details: Billing month, order description fields, number of device renewals, related renewal fee amount.

7.3 Core network monitoring & performance

7.3.1 NOC / GNOC

Sigfox has a two-level network monitoring level to ensure the respect of its obligations towards its channels:

- Each Sigfox operator has its own network operations center NOC for its territory base stations and infrastructure monitoring
- Sigfox ensures a level 2 monitoring through its global network operations center GNOC for all networks aggregated and the global cloud monitoring

7.3.2 Monitoring tools

The NOC and GNOC benefits from tools to:

- Monitor infrastructure.
- Manage the alerts provided via email or SMS.
- Fix issues remotely.
- Coordinate and manage the field interventions needed.

The metrics monitored can be related to hardware (cpu, disk, load, temperature …) but also to messages (delay, queue size, …).

7.3.3 Monitoring reports

Sigfox benefits from regular NOC & GNOC teams internal reports regarding their activity but also from a regular analisys of service level agreement (SLA) fullfilment.

8 Main workflows

This chapter describes the main workflows of the Sigfox infrastructure in order to illustrate the architecture with concrete use cases.

8.1 Device activation

In order to activate a device, there must be a device type created associated to an order. Then devices will be registered in the device type with their ID and PAC. When this is done the device is registered on the system and will become active after its first billable frame.

8.2 Message processing

Therefore, a Sigfox-ready device sends limited number of messages a day (maximum number is 140) with a short payload size (maximum size is 12 bytes) with a limited bitrate (in ETSI zone, 100 bits/s).

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

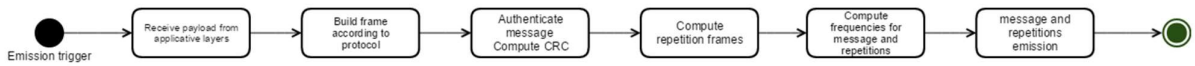


Figure 28: Device message emission process

Each message is received by one or several base stations that performs preliminary checks and relayed to the Sigfox Support System. Three (3) repetitions of the same message are made on different frequencies to maximize the chances of reception without error by the network.

When receiving a message from a base station (BS), the backend connected to the base station first check if the device is known or if the message had been transmitted in roaming (the device is in an area that is not covered by the Sigfox Operator it had been registered to).

- The CRA is involved to determined which backend is in charge of the device.
- The message is forwarded to this backend that makes the operations of non-roaming mode

In case the message had not been transmitted in roaming, the backend performs some verifications that are sum up below before delivering it to the application provider via a callback.

Note that if the device supports it and requests it, a response can be returned:

- Statically: the response is pre-configured in SIGFOX Cloud network
- Dynamically: the application provider provides the answer to be sent to the device in the callback response

There is no way to send an unsolicited message from the server to the device, the device always requests the bi-directional communication.

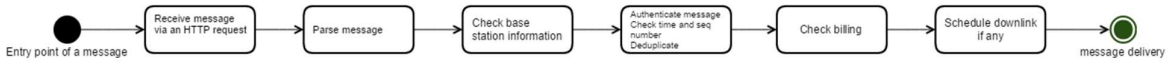


Figure 29: Uplink message processing

In case of bi-directional communication, the Sigfox Support System builds the response, authenticates it and evaluates the best base station to convey this answer. Some whitening and error correction codes are also involved. The following figure shows this Sigfox Support System processing to send this response to the device.

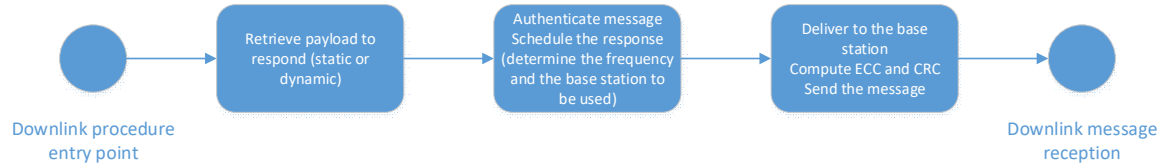


Figure 30: Downlink message preparation and emission process

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

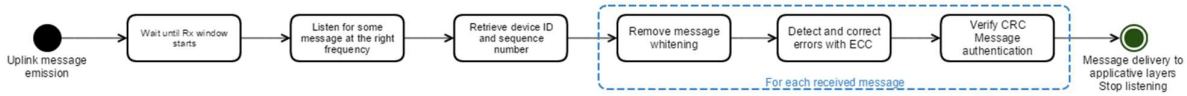


Figure 31: Downlink message processing by the device

9 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:

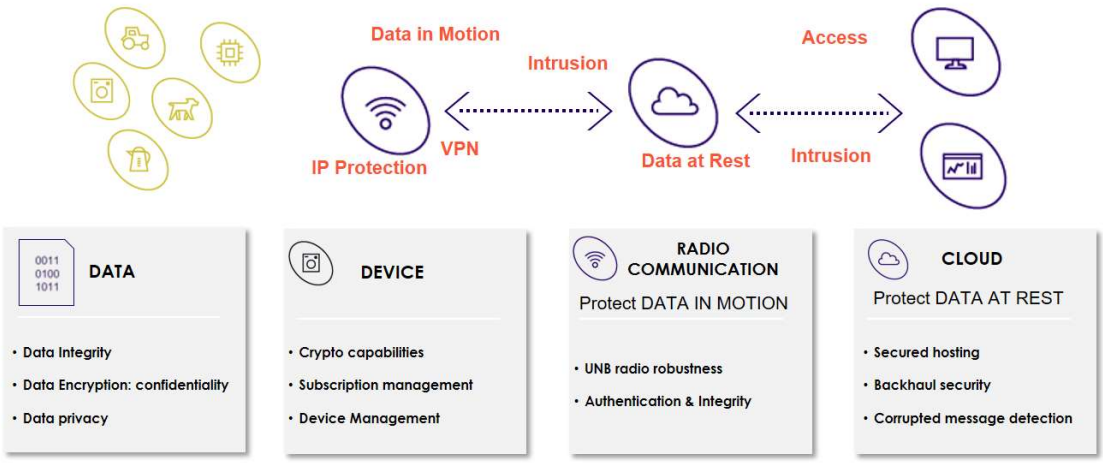


Figure 32: Security by-design & by-default

- 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 broadcasts a radio message. This message is picked up by several access stations and is 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 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 inside the Sigfox ecosystem as well as best practices and process ensuring integrity, availability and confidentiality of this data by respecting as well local regulations.

Since the key is unique per 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 TPM secure this entity. Sigfox Core Network stores Sigfox ReadyTM devices' authentication keys as well as traffic metadata. State-of-theart 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.

9.1 Security on message processing

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

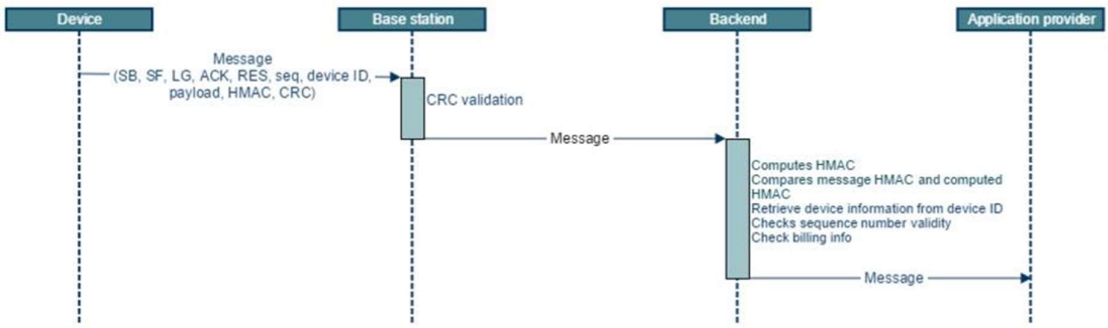


Figure 33: The different checks executed along the uplink message treatment

The following paragraphs detail the different mechanisms put in place.

9.1.1 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 / day, the sequence number shall be between 6 and 426 (6 + 3 x 140).
- If the subscription level is one message / day, the sequence number shall be between 6 and 26 (6 + 20) because 3 x 1 messages < 20.

9.1.2 MAC verification

Each device is provisioned during manufacturing with a unique symmetrical authentication key. 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) 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.

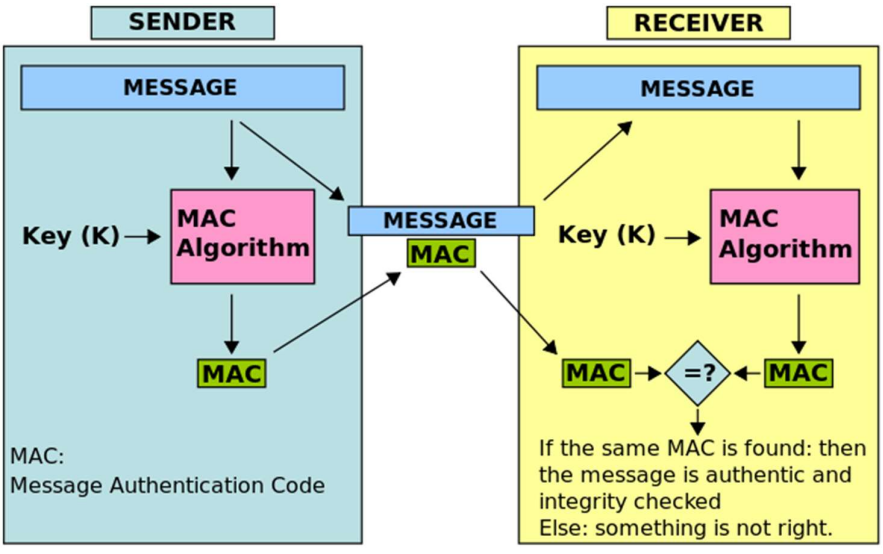


Figure 34: MAC verification to check the message integrity and device authentication

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.

9.1.3 Message Encryption

By default, data is conveyed over the air interface 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.

If the manufacturer wants to use encryption, it must indicate it on deviceType.

9.2 Security on base station & its communication

Base station can be deployed in hostile environment whereas it contains IP that shall be protected. Sigfox has integrated a Trusted Platform Module 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 as well protected by the TPM.

9.3 Security on key generation & provisioning

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

This process can be executed only if the corresponding manufacturer 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 the following:

- 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 *deviceID* range to the manufacturer for the given certificate and launches the generation. The 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 from the CRA the output files:
  - A binary file containing (device ID, key) pairs AES-ECB encrypted.
  - 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 *deviceID* in each module and optionally the initial PAC code.
- The application provider / end-customer receives from the manufacturer devices / modules with their *DeviceID* and their PAC.
- The application provider / end-customer accesses to the web portal of the Operation Support System in order to register the device by providing its DeviceID and its PAC to a Sigfox Operator.
- The Operation Support System checks in the CRA the DeviceID 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 to another Sigfox Operator.

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

9.4 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-ofservice (DoS), distributed denial-of-service (DDoS), reflective denial-of-service (RDoS), and distributed reflective denial-ofservice (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.

Chapter 3
End-customers Services Overview

sigfox

10 Connectivity service

This chapter presents the connectivity service provided by the Sigfox network to the end-customers and their devices.

10.1 Service overview

10.1.1 Service Scope

As described in Chapter 3, Sigfox offer a connectivity service to transfer devices messages to the customer application.

The environment implies devices, Sigfox base-stations, Sigfox Cloud and Customer Cloud that receives the callbacks.

Figure 35: Principles of the connectivity service

10.1.2 Global coverage and equal access

Sigfox Connectivity Service is based on the principle of global coverage and equal access.

Wherever a device is, it has access to the same connectivity service level as the one described in its contract. This is one of the main principles of our roaming management.

10.1.3 Roaming

Roaming means the emission or reception of a frame by an activated object on another Sigfox territory network called “the visited network” than the Sigfox territory network it has initially been subscribed on called “the home network”.

The roaming is processed by the OSS every 24h. The Roaming calculation is based on the time zone related to the activated object’s related BSS Order, mainly to manage roaming between different time zones. The reference date and hour is the reception date and hour at which a message is firstly received by the BS.

As per the definition above, if a message has been received by its home territory, there is no roaming even if the same message has been received by a visited network.

10.1.4 Whitelist and Blacklist

At order creation into the BSS, a channel can choose to whiteliste or blackliste territories. By default, all territories are whitelisted, which means that the devices are allowed to emit and receive frames to and from everywhere.

10.2 Commitments with SLA & SLO

Sigfox obligations for the connectivity service are defined through 2 service level agreements “SLA” and 2 service level objectives “SLO”.

The 2 SLAs are :

- **Uplink delivery time:** A message is delivered to the cloud in less than 1 minute in 98% of cases
- **Service availability:** The message transport service is available more than 99% of the time availability

The 2 SLOs are :

- **Portal availability:** Tools and API have a 99.8% of time availability.
- **Support service:** There are 3 levels of incident priority with a measured time to take into account, time to solve and communication update (cf. section 21).

11 Spot’it - Geolocation service

Sigfox offers the first GPS-free IoT location service based only on its technology available globally. Sigfox Spot’it service is available for all devices equipped with only a Sigfox Verified module. No need to retrofit, no need for specific update in the hardware or the software: Sigfox can now provide a location for all existing and future devices all over the world.

11.1 Service overview

11.1.1 What is Sigfox Spot’it service?

For each message sent by a device, Sigfox Spot’it provides in real-time the coordinates (latitude/longitude) and the precision of the location in km, delivered through a callback or a standard Sigfox API. Spot’it also includes a map showing where are the fleet of devices.

As for all services provided by Sigfox, this service is:

- Low power: No need of GPS chipset, no need of specific hardware, no additional processing.
- Cost efficient: No hardware extra cost, no extra message to be sent by the device.
- Simple: The location of the device is directly sent to the customer IT through a callback or through standard API.
- Global: Location service is available for all Sigfox territories.
- Indoor and outdoor: Sigfox Spot’it is available anywhere covered by the Sigfox Global Network.

The Sigfox Spot’it service is available in all countries covered by the Sigfox Global Network. It does not require any specific capabilities on devices. It can be enabled on any devices connected to the Sigfox network.

The service availability and its accuracy depend on the location of the device. A heat map provides the availability of the service and the estimated accuracy depending on the location. This map is regularly updated and it is available on the Sigfox Spot’it website.

11.1.2 Information provided

For devices that have the Sigfox Spot’it service activated, and for a single message reception, the system provides an estimation of localization coordinates accompanied with a radius. The radius corresponds to the accuracy of the location information.

Figure 36: Information provided by Sigfox Spot'it service

11.1.3 Location computation principle

The location computation is based on the data from the Sigfox infrastructure, coming from the several replicates of the same messages sent by a device and received by different base stations.

Those different replicates in addition to the message itself have additional information coming from the network such as:

- The identifier of the base station that received the message.
- The RSSI (Received Signal Strength Indicator) that is an indication of quality for the signal received.

The method used is based on the signal strength from the RSSI with a probability model.

- With the identifier, the Sigfox infrastructure is able to define the location of the base stations.
- Based on this information of base stations location and signal strength, probability functions are computed for each location.
- The location with the highest probability is selected.

This approach allows for the first release of the Sigfox Spot'it service to have an accuracy in km, depending on the base station density in the considered territory. The computed location is then given in latitude, longitude and radius.

11.1.4 Service enablement

The activation of the Sigfox Spot'it service is executed in 2 steps:

- The service enablement at the subscription order level.
- The service activation at the device type level.

The initial step aims at making the Sigfox Spot'it service available for a subscription order. The procedure to execute depends on the ordering management process used by the Sigfox Operator or the Channel:

- If the ordering management is done through the Sigfox OSS portal, Sigfox Operators enable the service from the same web interface on new or existing orders.

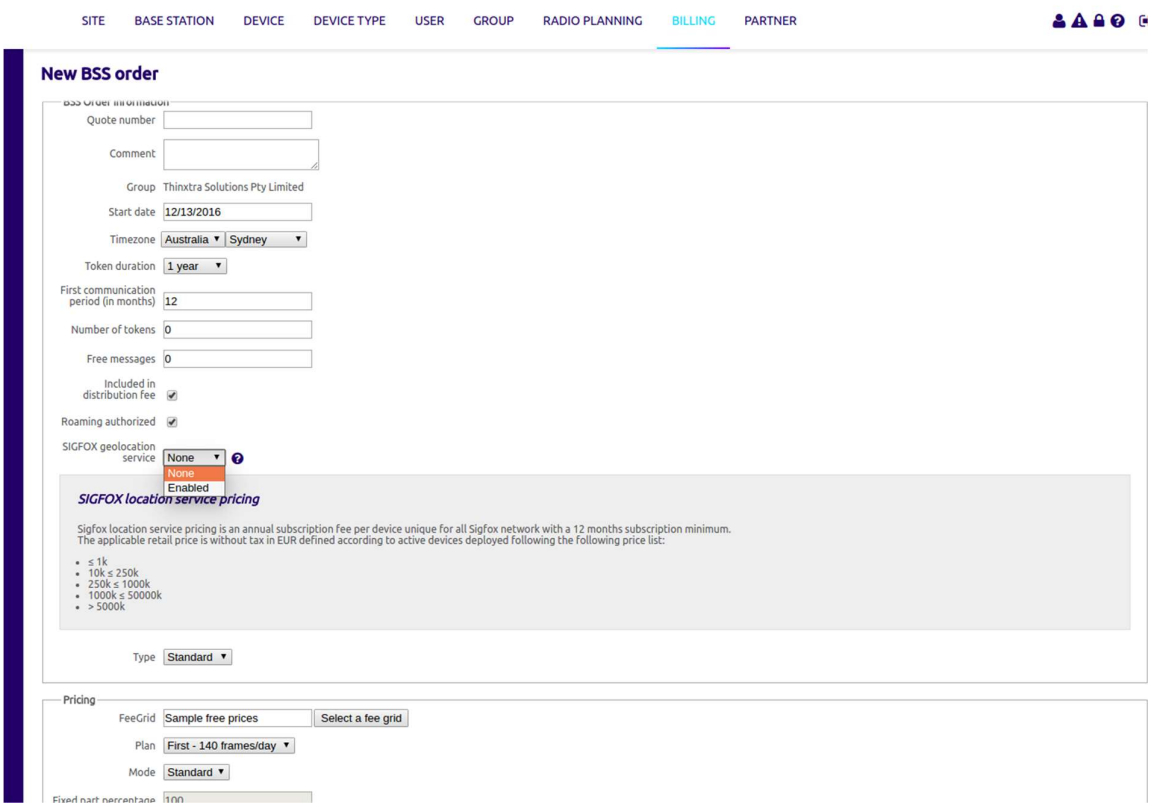


Figure 37: Spot'it service enablement through Sigfox OSS portal

- If the ordering management is done through the Sigfox Connect Contracts portal, Distributors and Channels will use the same interface from April 2017: They will be able to submit quotes and to pass orders with the *Sigfox Spot'it* service enabled.

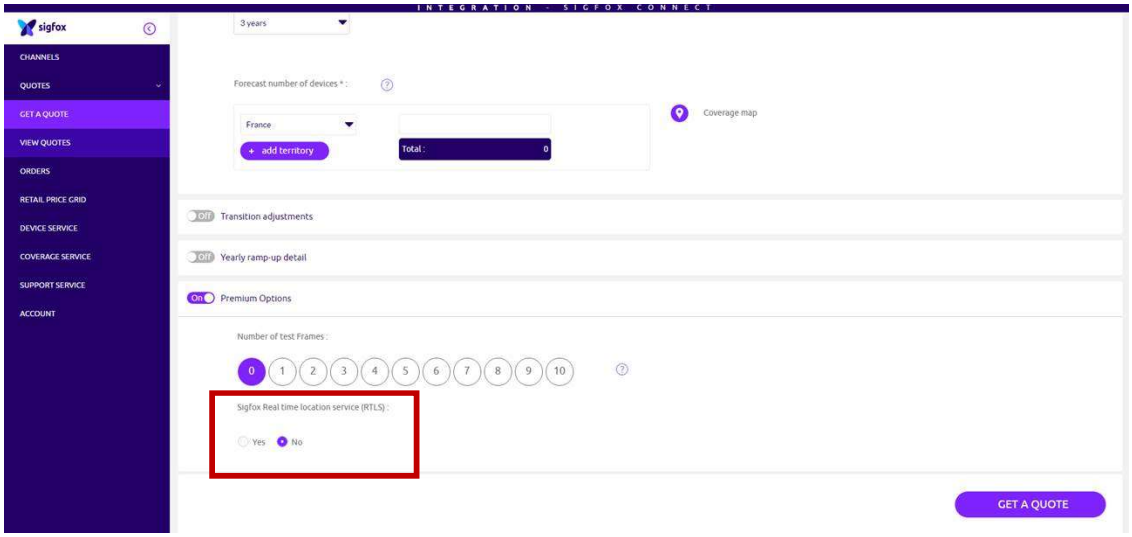


Figure 38: Spot'it service enablement through Sigfox BSS portal

In the meantime, they will be able to enable the service on a specific order by submitting a support ticket to the Service desk. The service enablement on an existing order will be available under Sigfox Connect Contracts portal later in 2017.

11.2 Commitments with SLO

Dedicated Service Level Objectives (SLO) have been defined on a quarterly basis:

- **Sigfox Spot'it Data Accuracy per Network** defining the accuracy of the service on messages: 80% of messages' location has an accuracy lower than 20km.
- **Sigfox Spot'it Success Rate** defining the percentage of messages with a location information (whatever accuracy) where the service is available: 90% of (single) messages emitted have a location information.
- **Sigfox Spot'it Availability** defining the general availability of the service at Sigfox infrastructure level: 99%
- **Sigfox Spot'it Delivery Time** defining the average duration to receive a Sigfox Spot'it callback from the message emission by the device: 3 minutes for 98% of Sigfox Spot'it callbacks.

Chapter 4

Integration to Sigfox Ecosystem

sigfox

12 Access to Sigfox ecosystem

The Sigfox ecosystem includes different players within the Internet of Things value chain which are Certified and/or have signed an agreement with Sigfox such as technology enablers, solutions enablers, device makers, design houses etc.

Through the ecosystem portal mentioned in the next paragrpah, Sigfox will facilitate the access of Channels to its ecosystem and the visibility of the Channel within this ecosystem. The ecosystem portal is publicly accessible and personal accounts may be created.

The main features provided by the ecosystem portal to the Channel are:

- **Public Company page**: The Channel will get a page on the partner network where it will be free to present the company and its positioning in IOT.
- **Public Product page**: The Channel will be able to create an unlimited number of product pages, each with a description of the proposed solution. These pages typically contain text, availability details, photos, technical characteristics, certification status and links to the Channel websites.
- **Search engine**: All the browsable content will be indexed and searchable from the ecosystem portal. Filtering per multiple subcategories also simplifies access to the right information to the site visitor.
- **Conversation**: A visitor of the portal may start a live conversation with the site moderator in order to obtain guidance about the portal and its content.
- **Moderated Contact Request**: A visitor of the portal may click on the provided buttons in order to request contact with the Channel. In that case, the contact request will be routed to a Sigfox moderator who will then pass it on to the Channel designated contacts.
- **Email notifications**: A visitor of the portal may request regular notifications to be sent to him/her in case of changes to a given category or page.

Sigfox is constantly improving its ecosystem portal, and as such the list of features may vary.

As of January 2017, the URL of the ecosystem portal is https://partners.sigfox.com and its current implementation is pictured below.

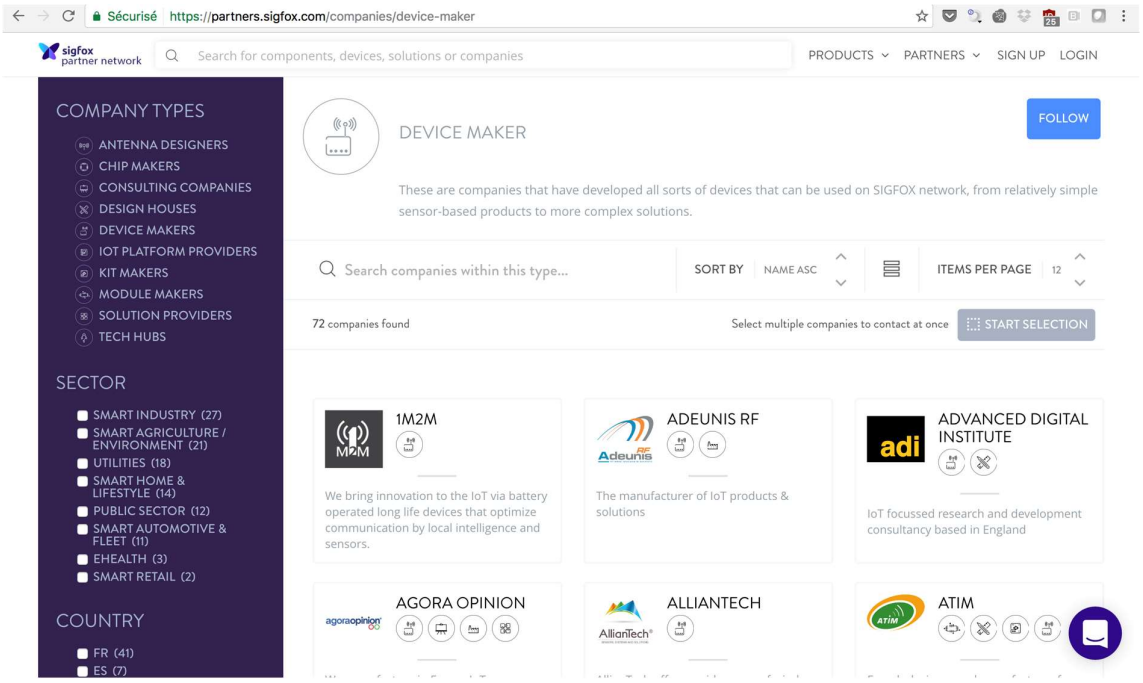


Figure 39: The Sigfox ecosystem portal

13 Partner enablement

Sigfox makes available training sessions in order to enable the Channel to understand the specificities of the Service and therefore promote and sell their Global Offer as well as support the clients.

The Parties shall plan for on-boarding sessions that will provide the initial training to Channel teams.

13.1 Training program

The training sessions to Channel can be delivered according to the following formats:

- **Digital learning program (Sigfox Academy):** it is composed by standard training modules for sales, pre-sales and technical support teams, available on-line. The Channel can create as many accounts as needed on this platform.
    - Modules are constantly being added to the platform, and existing modules are updated as soon as it requires. Some modules are available in order to understand the Sigfox offer, its technology and the tools that are available to the Channel.
    - Some of the modules are also aggregated into Learning programs suitable for specific functions at the Channel.
    - Depending on the modules, some can provide self-evaluation mechanisms such as quiz or post learning tests.

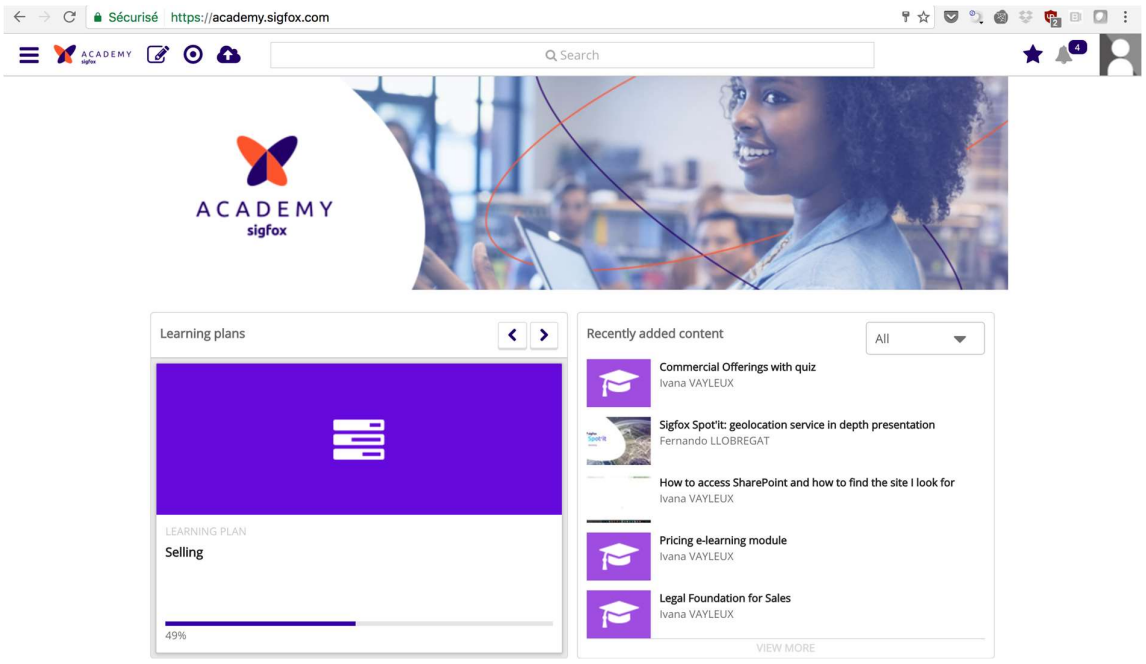


Figure 40: Digital learning program on Sigfox Academy website

- **Instructor-led training** (online or on-site sessions): A session ran by an instructor specifically for the Channel. The appointed Channel Partner teams (marketing, pre-sales, sales, technical and support) will be trained by Sigfox within a time frame to be agreed between the Parties. If necessary, these sessions will be customized to match the focus markets focus (territories, verticals, applications) and other requirements specific to the Channel. Sigfox can provide such session up to once a year to the Channel in a location chosen by the Channel.

13.2 Training certification program

It is the intention of Sigfox to provide certification programs for both customer facing teams as well as for technical support teams. The certification will be based on the evaluation of the good understanding of Sigfox's key messages, its unique selling points and the specificities of its technology.

The programs are currently under development.

14 Pre-Sales support services

Sigfox can make available pre-sales support to Channel over a digital platform. The pre-sales support includes elements such as FAQ, marketing and technical collateral as mentioned in the next paragraphs.

Sigfox can assist Channel with on demand support, upon quote accepted by Channel, for specific requirements (e.g.: coverage extension, new device and new platform to be certified).

Sigfox will provide the Channel with a certain number of support services in order to assist the Channel with its development of the usage of Sigfox's network.

- **Ask.sigfox.com**: this public digital platform is meant for technical questions to be asked. Several Sigfox experts and some community members constantly look for unanswered questions and provide best possible answers. There is no SLA for this platform, all questions and answers are public. The platform can also be searched and acts as a knowledge database.

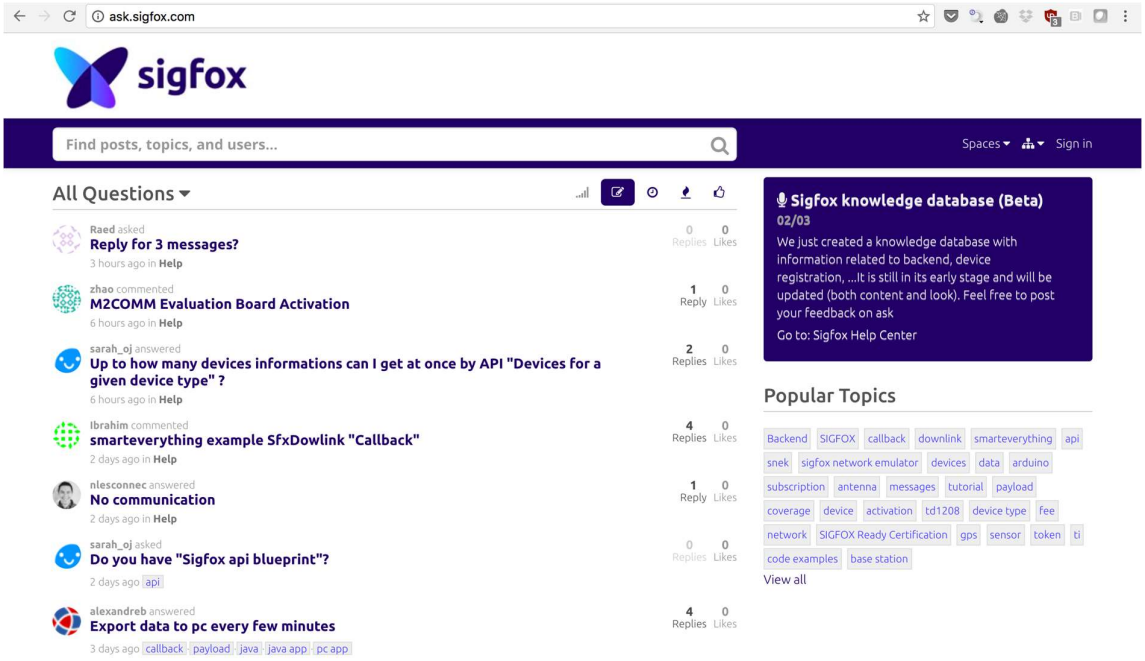


Figure 41: Ask.sigfox.com site dedicated to answer to Channel's questions

- **Sigfox Support**: Through the regular support interfaces, Sigfox also answers technical questions related to specific customer solutions. The Sigfox support can look upon topics such as backend, API integration, coverage, Sigfox technology… Support can be queried through its ticketing system or by phone. The responsiveness of the support is monitored and subject to SLA/SLO as described in the SLA chapter.
- **Presales Support**: The Channel can make request to its channel manager for specific Presales Support for a given deal. Sigfox team will review the deal and will propose to the Channel a support program fitted to the requirements and

suited to Sigfox availability. In some situations, Sigfox may not be able to match the requirements and decline the request. The support program may include resources such as Sales Engineers, Channel managers, Program managers, … These resources will be free of charge for the Channel. Specific timelines and scope of work will be defined jointly at the initiation of the program. The typical tasks managed by these resources are writing specific customer collaterals, attending customer presentations, providing guidance in Sigfox's ecosystem…

- **Professional Services (PS)**: Beyond and above the Presales Support that can be offered, Sigfox can also provide support to the Channel with paid-for resources. These resources may be Sigfox employees or qualified third-parties. The PS will work per a detailed Scope of Work to deliver key elements of the solution. These elements may be an object design, antenna design, technical recommendation, industrialization program, project management, … The terms and conditions as well as the pricing schedule will be included in the Scope of Work. The mission will begin after the Channel explicit agreement and signature of the SoW.

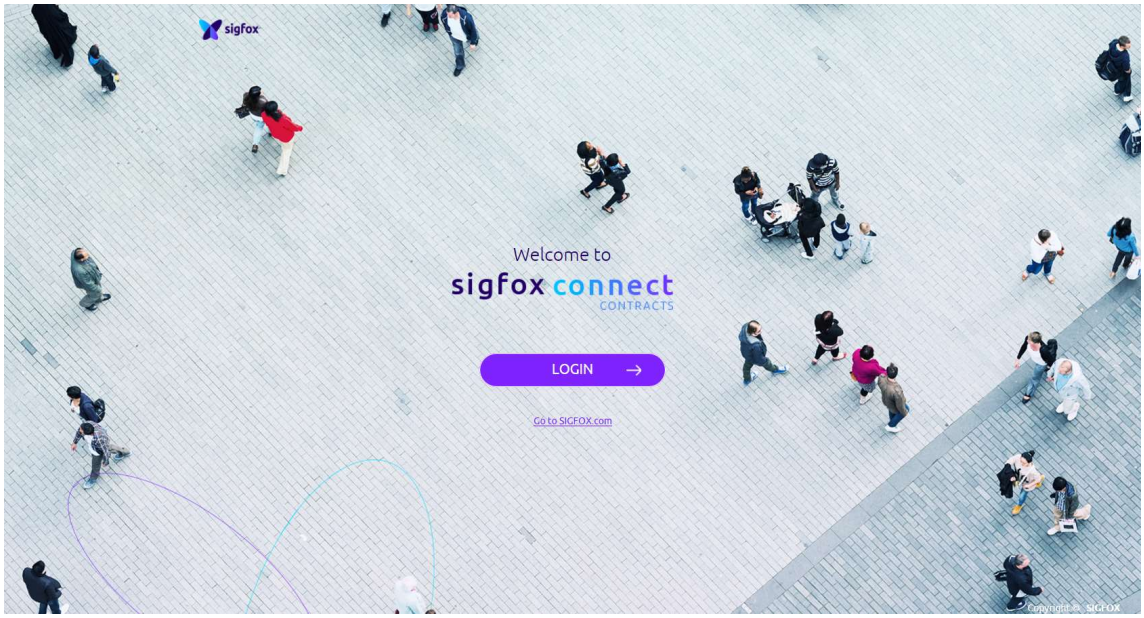
15 Collaterals & demonstration

Sigfox provides the Channel with a global repository for all the documentation, including collaterals and demonstration walkthrough. The repository is currently provided with Microsoft Sharepoint (subject to change).

Chapter 5
Sales Tools Overview

sigfox

16 Connect Contracts platform overview



16.1 General overview

The Connect Contracts platform enables Channels to create and manage on their own Quotes, Orders, and Groups of users. Channels partners will automatically access information needed to bid, transform contract and manage service subscriptions, enabling their own customers to access the SIGFOX global network with one single Contract. A Channel can create tailored offers for each client while taking advantage of pooling large volumes of devices.

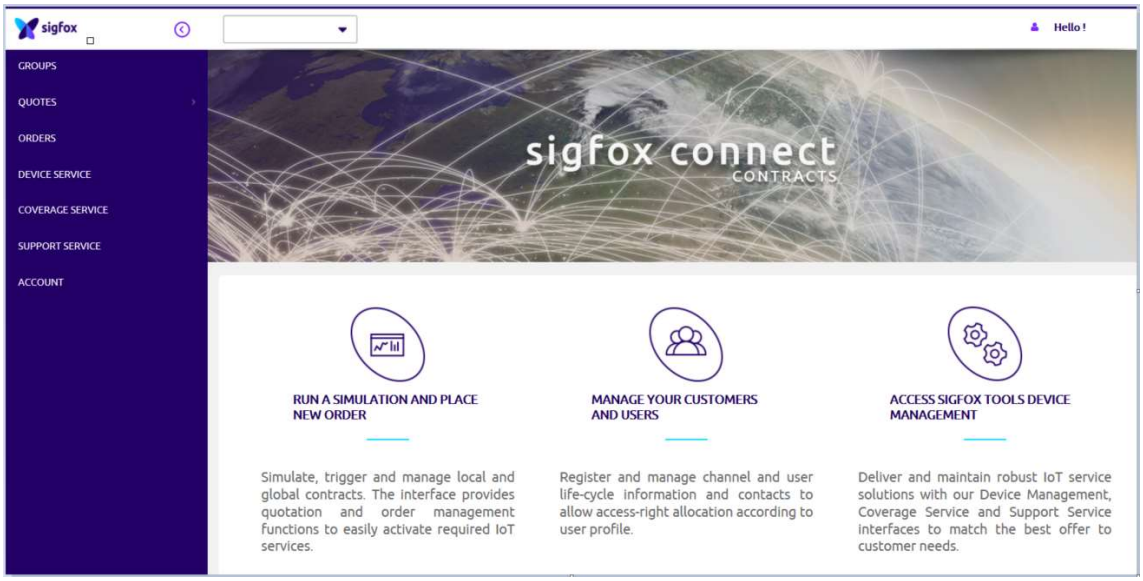


Figure 42: Connect Contracts landing page

16.2 Create & manage quotes

A quote compare pricing per subscription plan for a determined number of hypotheses, which includes the subscription duration, the number of objects per country and service level.

Channels can also be assigned quotes from their Distributor.

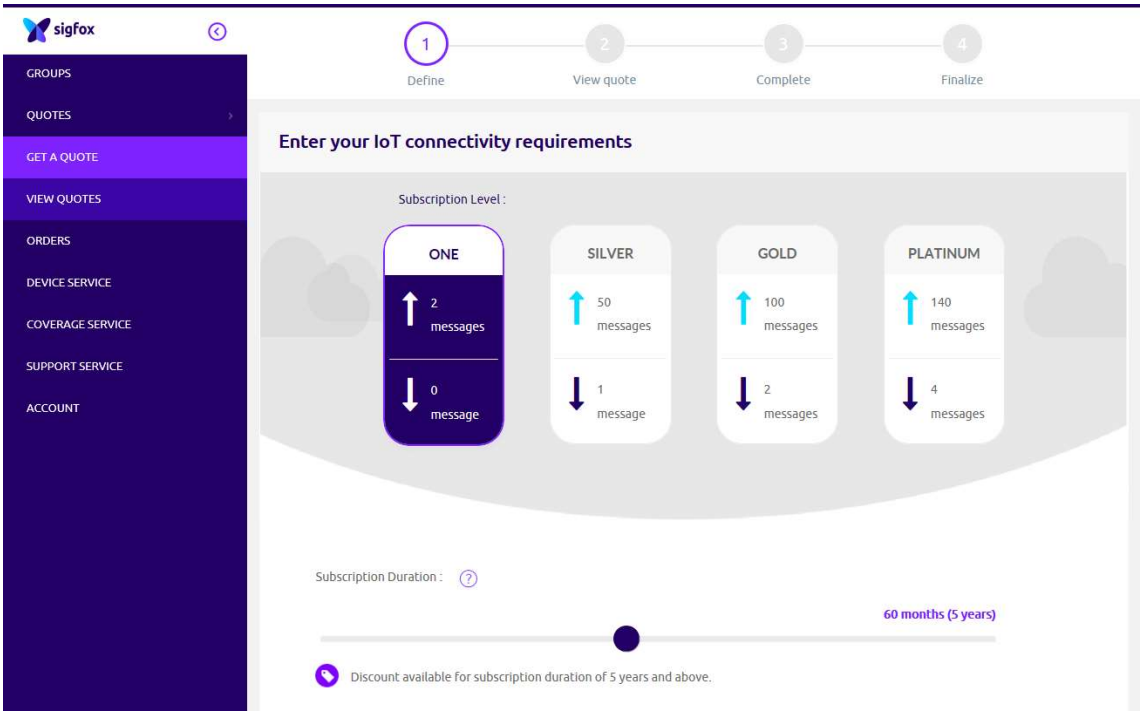


Figure 43: Subscription level definition

The path follows four steps (two as quote and two as order)

- **Define**: set the hypotheses to simulate the quote

In this step the Channel Partner choose:

- ✓ the subscription level (i.e. the number of messages an object can emit up to and receive each day). There are four levels: One, Silver, Gold and Platinum.
- ✓ the subscription duration (i.e. the number or months each object will use the connectivity, from 12 months to 120 months (10 years)).
- ✓ The territory or territories where devices will be deployed
- ✓ The number of devices to de deployed on each territory. A minimum forecast of 100 devices is expected.
- ✓ Premium option: test frames and geolocation (Spot'it)

- **View quote**: review the proposed pricing per object and in total and possibility to save quote

In this steps the Channel Partner can compare pricing plans: **Committed volume**, **Flexible Committed Volume** and **Pay As You Grow**. In the section "price per device" the results are presented separately for each country and per service plan, with the adequate currency.

The quote parameters can be modified until the quote is saved with a reference number.

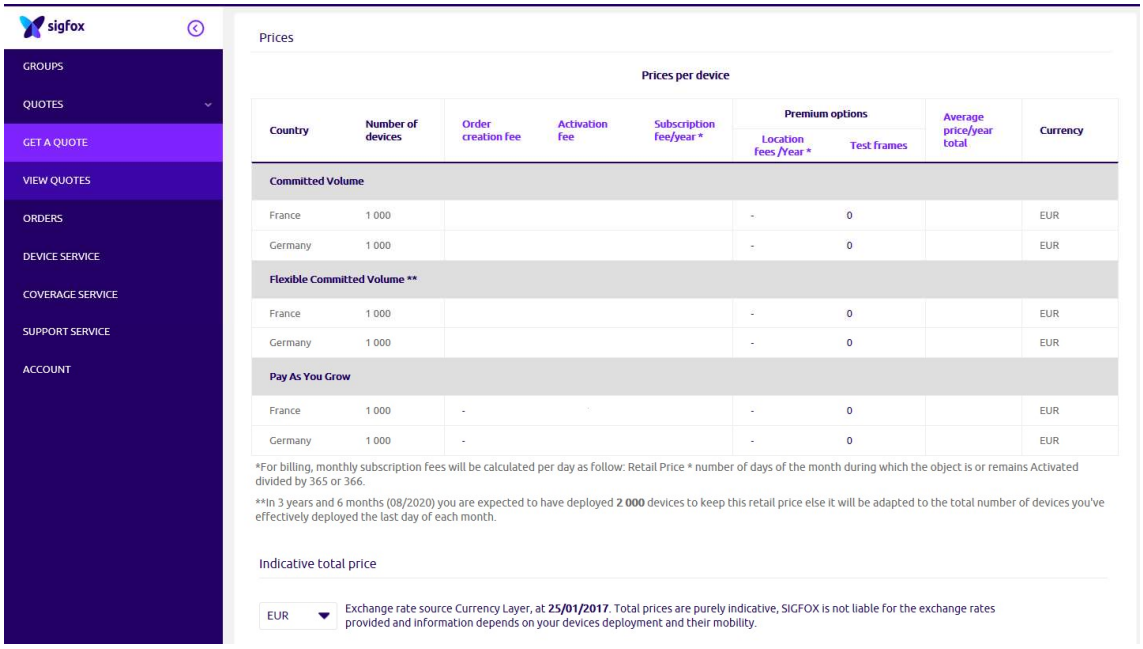


Figure 44: Quotation results

The last two steps are details in the section below.

16.3 Create an order and manage mobility

- Once the quote is saved, it is possible to proceed it to an order.

- **Complete**: upon acceptance of a quote, complete the mandatory fields

When the Channel Partner wants to convert a quote into an order, the selected quote needs to completed with the option of automatic renewal and global mobility which set country lists where the device can or cannot operate (white and black list).

- **Finalize**: review order specifics and confirm it

Once the order is confirmed, it gets automatically a reference name that will be used in the OSS Portal.

16.4 Administration

16.4.1 Group management

Groups can be customers or also used to help managing deployments in the OSS Portal.

Customers can be managed by simply clicking on Groups from the main menu. This will display the list of groups that belongs to the Channel, with the possibility to create more groups. Information available include name, description and users assigned to the group.

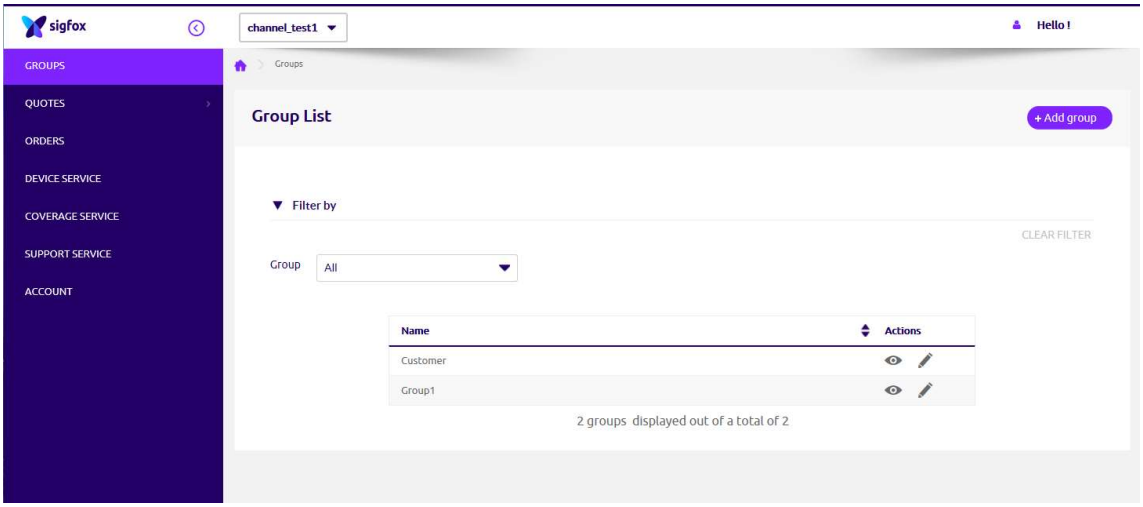


Figure 45: Group management

Group (Customer) users don't access Sigfox Connect Contract, but use the BSS-OSS web site https://backend.sigfox.com.

16.4.2 User management

User management is done through the account view. The first tab gives the account details such as Legal name, Commercial name, time zone, Channel Partner Agreement (CPA), address and contacts.

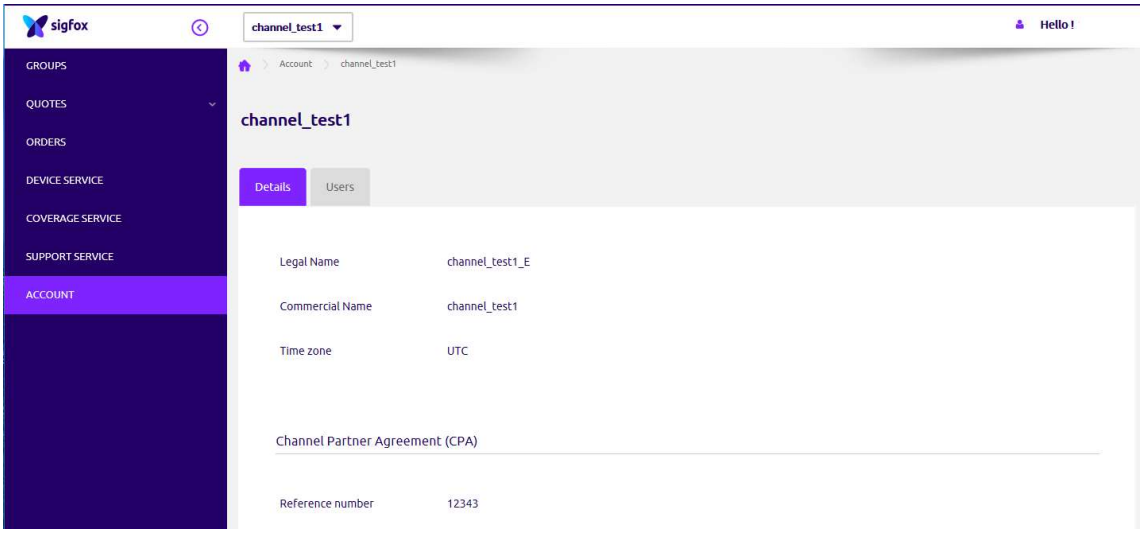


Figure 46: User management to access to Connect Contracts platform

Users with administration right can add, edit, delete users and proceed password reset. Users may be assigned different roles defining the visibility and permissions they have to operate specific features on the portal.

In Sigfox Connect, there are 3 user roles for Channels and 1 role for prospect channels:

- **ADMIN** role is for the Channel user in charge of user administration for the account and also for support. This should remain a restricted role.
- **SALES** role is for sellers, for people creating quotes and orders for customers.
- **QUOTE** role is for people simulating and creating quotes, but cannot place orders.
- **PROSPECT** role is limited to simulation, without the possibility to save quotes.

17 Service coverage tools

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

17.1 Service coverage public access

On the Sigfox web site www.sigfox.com there is a link to coverage map:

http://www.sigfox.com/coverage

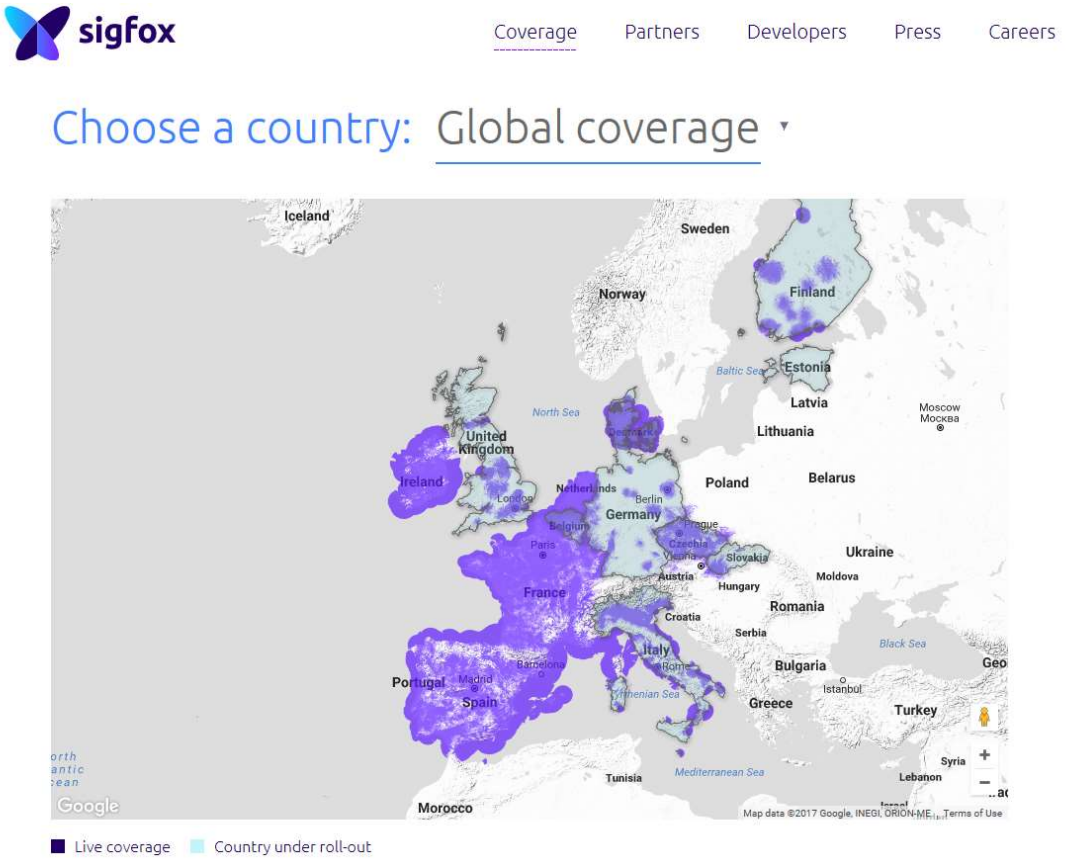


Figure 47: Global coverage map under www.sigfox.com web site

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

17.2 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:

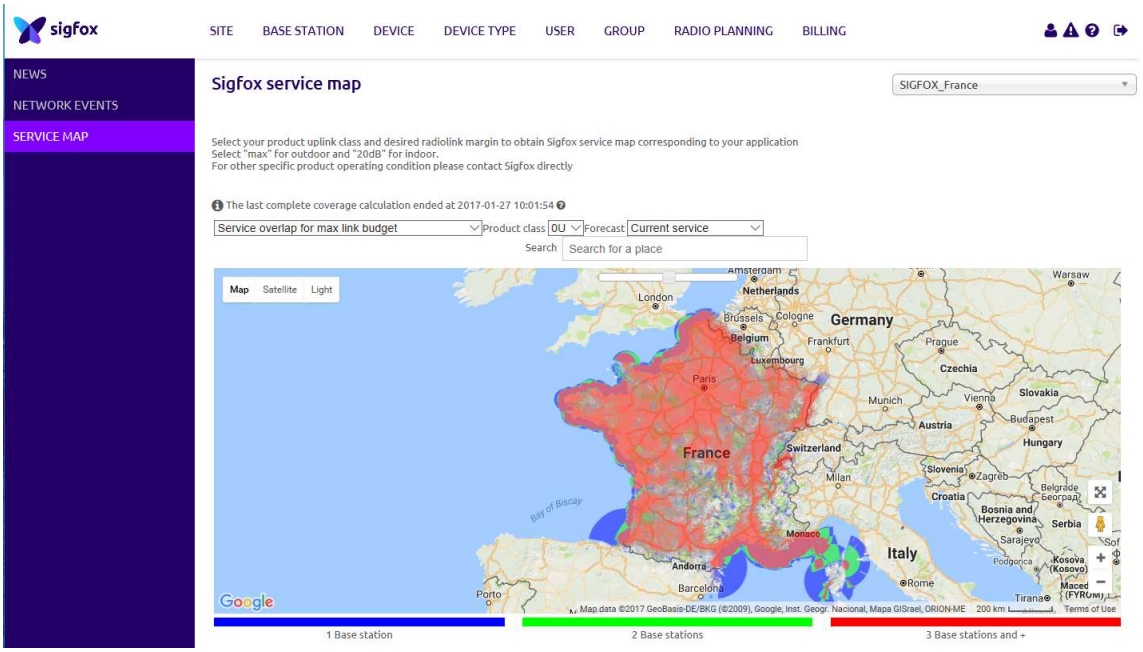


Figure 48: Service map integrated to OSS portal.

17.3 Global Coverage API

A new API is being developed and will be accessible to all OSS Portal user (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.

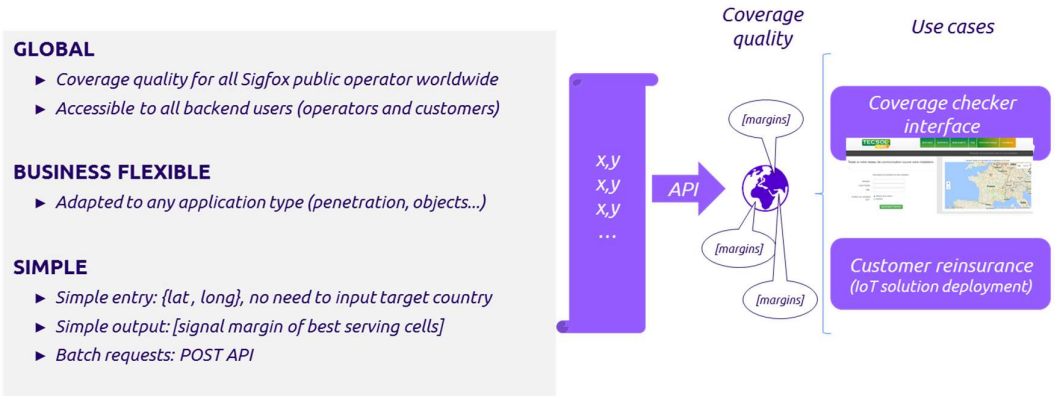


Figure 49: Global coverage API to evaluate the network coverage on different locations

Chapter 6

Operations Tools Overview

sigfox

18 Device management

This chapter presents the device management features and processes to provision and to activate devices. General overview

18.1 Notion of device and device type

Every device has a unique and permanent ID embedded in the device itself. Each device has also a unique property title with the PAC (Portability Authorization Code).

A PAC is allocated to the owner of the device. This PAC value changes as soon as the device is registered in the backend. Then, when a device is bought from the production line, it comes with an ID and a PAC provided by the reseller. Once the device is registered in the backend, a new PAC will be generated and available in the backend. If the device is to be sold again, the owner will need to provide this new PAC.

A device type is a group of device with the same behavior. A device type belongs to a single group and is linked to a single order. A device type defines as well the callbacks to retrieve messages.

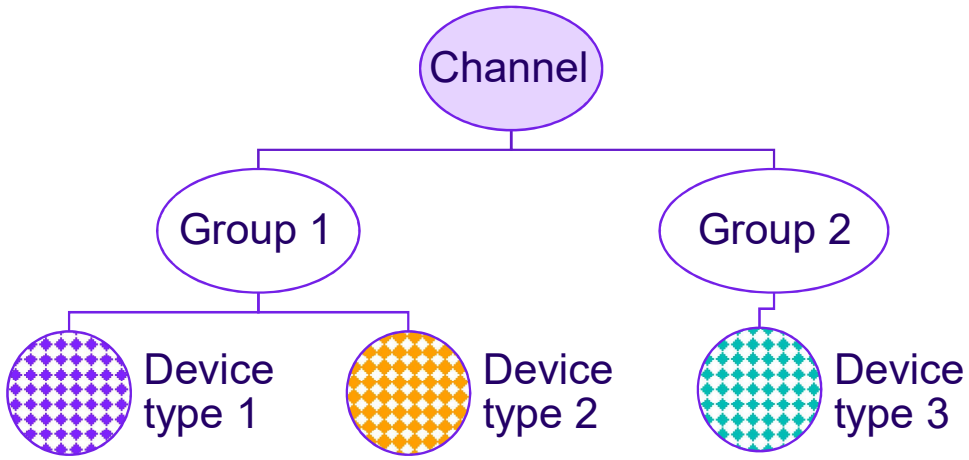


Figure 50: Hierarchy of device type creation

Channels allocate orders to Groups and possibly to device type. Groups allocate order to device type in their group or in sub-groups.

18.2 Provision and device activation

First step is the device type creation in the OSS Portal:

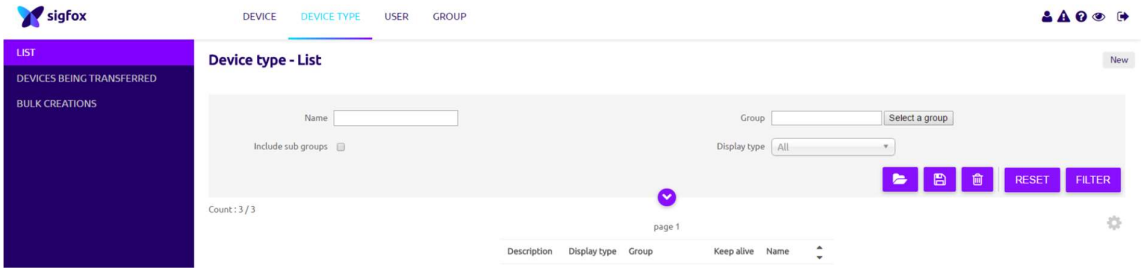
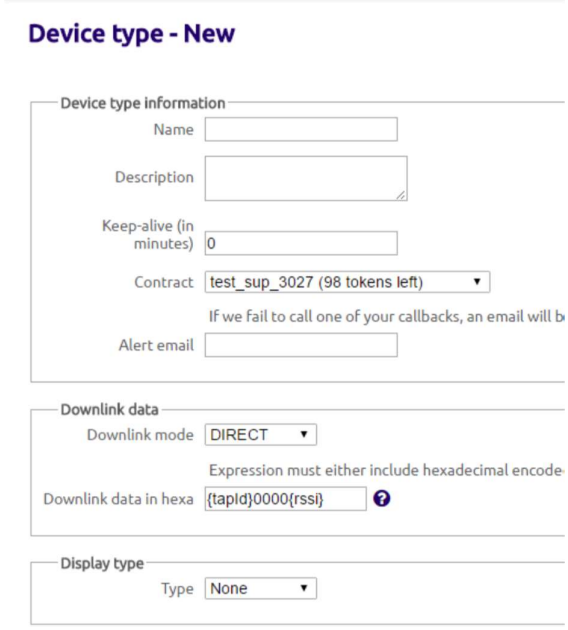


Figure 51: Device Type management

- On the Device type tab click on new.
- Select the Group managing the device type.
- Enter the device type information:



The contract cannot be changed once the device type is created.

Figure 52: Device Type creation

When the device type has been created, they are 4 ways to register devices:

- “New”: Register devices one by one / move device from a device type to another (different contract).
- “New series”: Register batch of devices / move devices form device type to another (different contract).
- “Edit series”: Edit device information / move devices from device type to another (same contract).
- “Replace series”: Replace broken devices by new ones.

It is possible to monitor devices on the device tab: A list of devices displays average Rssi, average SNR, communication status, device type, device id, last seen date, name and token state.

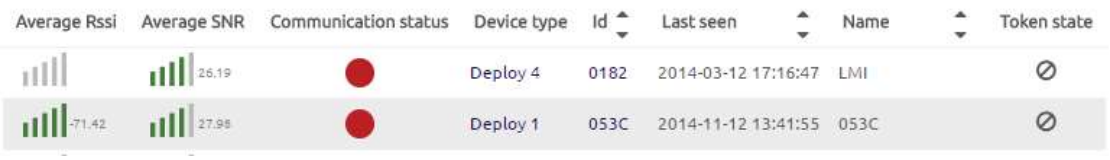


Figure 53: Device information in the device list.

To check the messages for a device, click on the ID and “Messages” on the left hand side menu. The list of messages received by the backend is displayed.

Chapter 7
Operational Processes

sigfox

19 Support Service

Every Sigfox Operator in the world has its own Service Desk. A Channel might decide to submit a support request to a specific Sigfox Operator Service Desk depending on the territory where it runs his business activity.

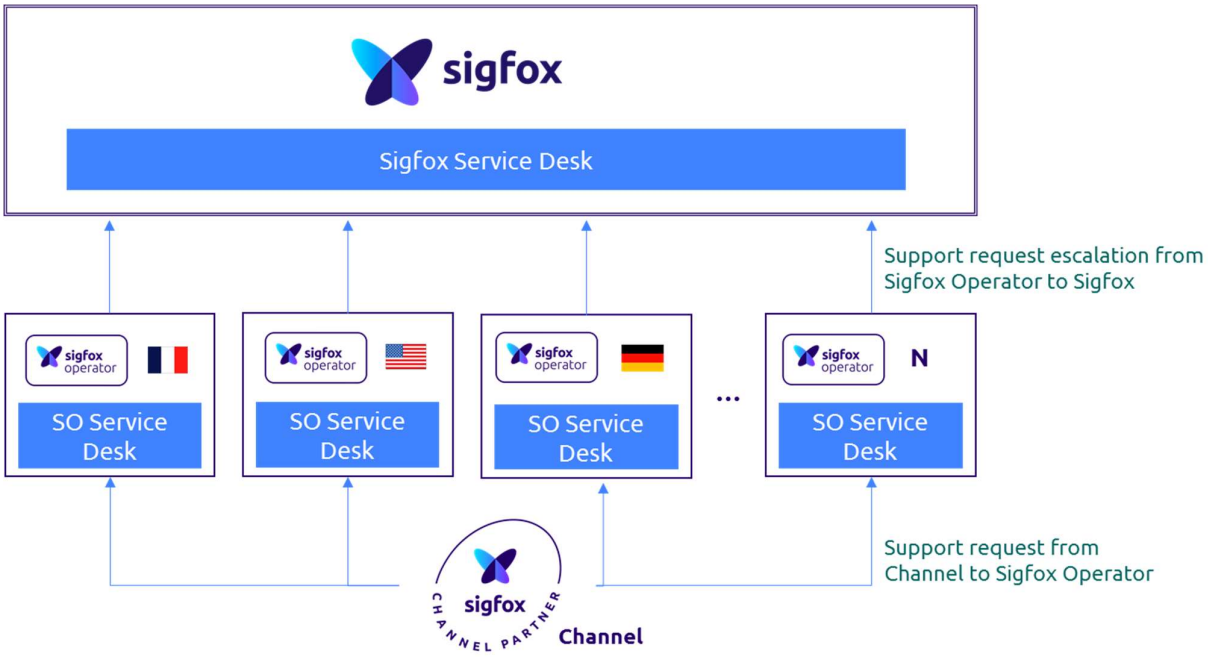


Figure 54: Support request processing between Channels, Sigfox Operators and Sigfox

The Sigfox Operator Service Desk shall provide Level 1 support to the Channel in English or in the local language. If the local Service Desk is not able to resolve the request, it shall request Level 2 Support to the Sigfox Service Desk.

In order to enable an efficient support service, the request processing between Channels, Sigfox Operators and Sigfox is performed on a unique ticketing tool.

20 Support portal

The Sigfox Operator shall grant the Channel access to the Support portal. The support portal provides a friendly-user GUI where the Channel shall submit support requests.

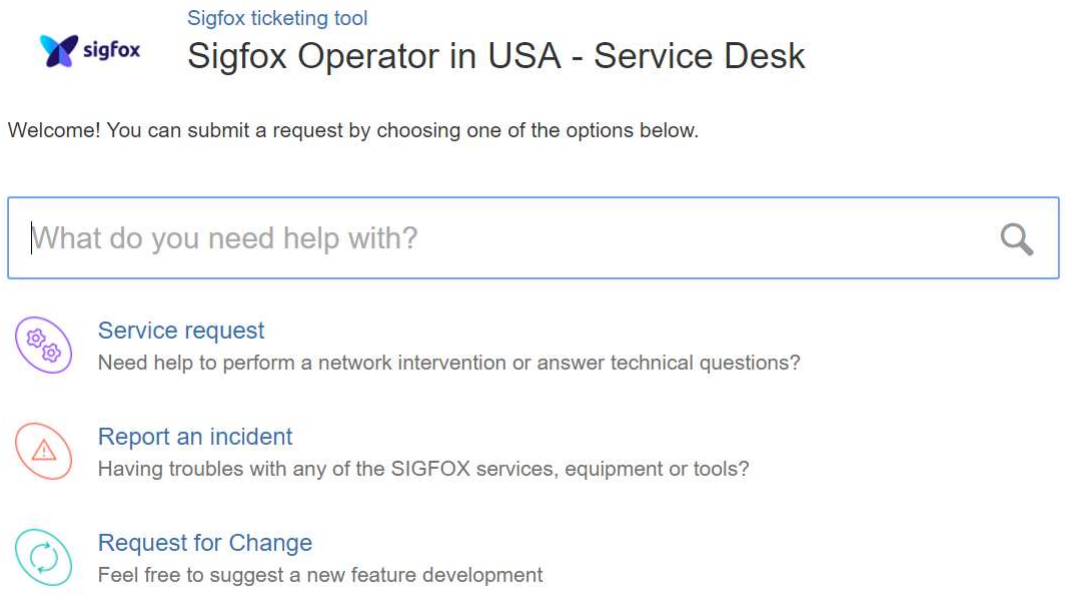


Figure 55: Support portal GUI

The Support portal includes a search-bar where the Channel can look for troubleshooting articles.

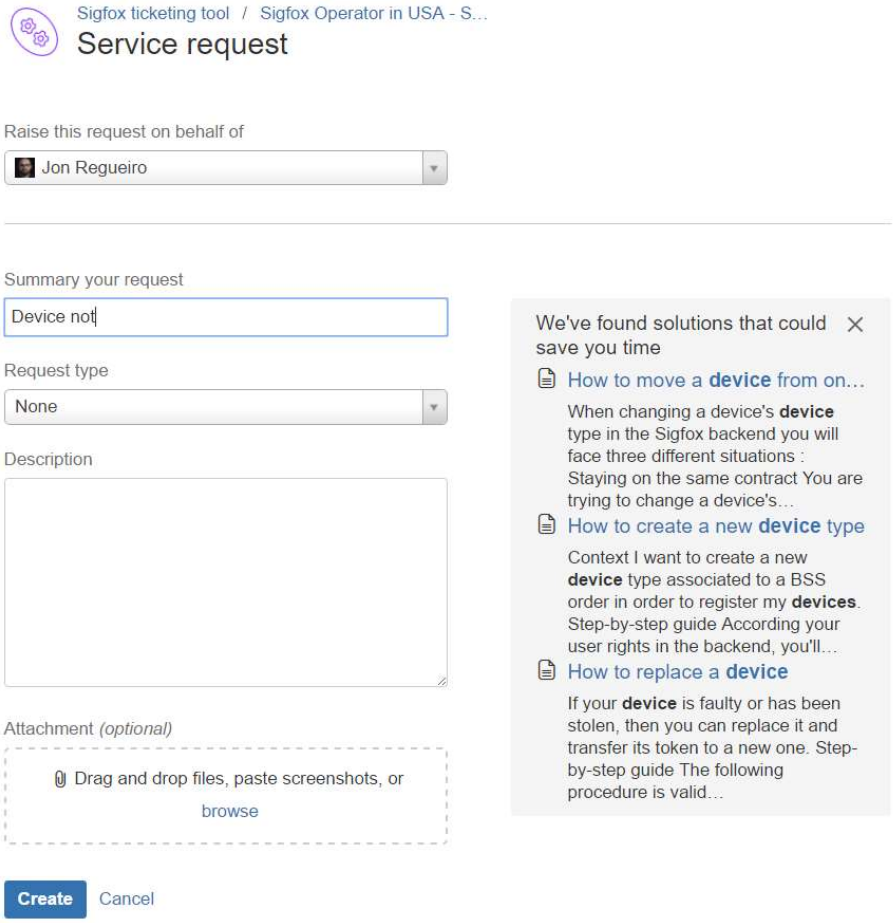


Figure 56: Service request creation

In the same manner, the portal suggests related articles when a support request is being created.

Support portal users shall also follow-up all ongoing support requests between the Channel company and the Sigfox Operator via a Dashboard

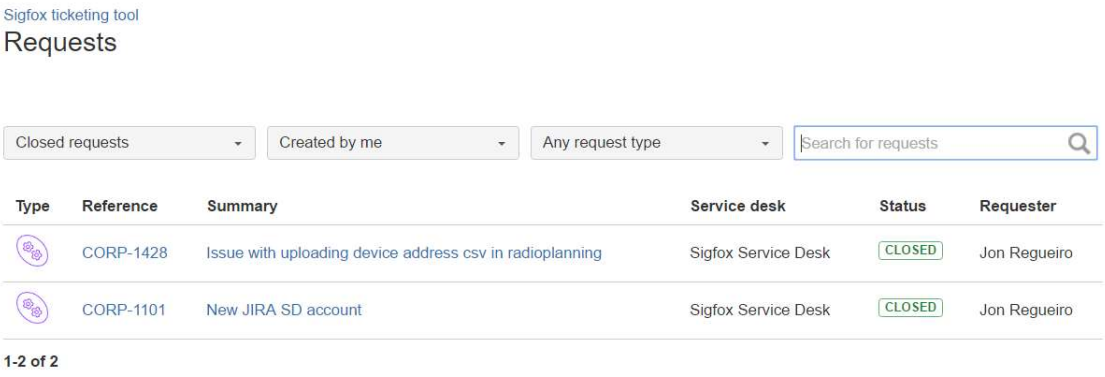


Figure 57: Support portal user dashboard

When choosing a request, the user shall see the requests status, as well as all the exchanges between the Channel and the Sigfox Operator Service Desk.

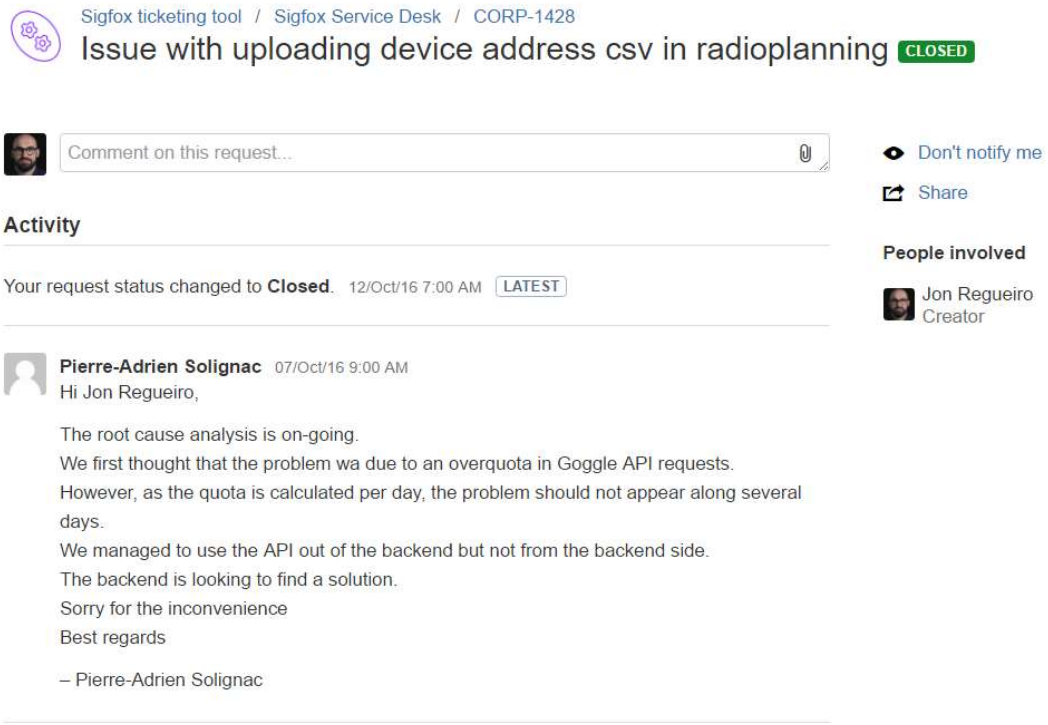


Figure 58: Request overview

21 Incident management

The Incident management deals with any event which interrupts or degrades Sigfox Operator Services. Incident can be reported by different entities:

- Channels to the Sigfox Operator through its Service Desk.
- Sigfox Operator to Sigfox Corp through Sigfox Corp's Service Desk.

Incidents can also be proactively reported by Sigfox Operator's NOC (Network Operation Center) or by Sigfox Corp's NOC & Cloud monitoring.

Note: Service requests will be handled as a particular type of Incidents that do not interrupt or degrade Sigfox Service(s). Those requests will be handled through Incident management process (and dedicated tools).

21.1 Incident status & priority

- **Incident status**

An incident can have the following status:

- New: A unique identifier has been associated to the incident.
- In progress: Incident is being processed by Sigfox Operator.
- Waiting for customer: Sigfox Operator awaits information from Channel.
- Resolved: A workaround or definitive solution has been implemented.
- Closed: Channel has validated incident resolution.

- **Priority details**

The following table describes the different level of priority for an incident with the business impacts:

Priority	Description of Incidents	Business Impact
P1 Critical Service Affecting	100% of the Channel's objects received messages cannot be made available to the Channel according to the service level agreement.	*Critical impact on ability to operate business processes.*
P2 Major Service Affecting	Between 5% to 99% of the Channel's objects received messages cannot be made available to the Channel according to the service level agreement	*Significant impact on ability to operate business processes.*
P3 Minor Service Affecting	A minor degradation of the Service or some functionality that causes minimal loss of Service and does not limit its critical functions.	*Minor impact on the ability to operate business processes.*
Request Non Service Affecting	No limitation of the Service (examples are notifications about faulty documentation, questions or requests for improvement).	*No impact on the ability to operate business processes.*

Table 1: Priority level definition for incident

21.2 Timescale to manage incidents

Timescales are defined as below:

- **Time to take into account (TTAC)**: Elapsed time between the timestamp of an Incident Ticket creation in the ticketing tool (unique ID has been communicated to the entity who reports the incident) and beginning of effective work on this incident
- **Time to solve (TTS):** Elapsed time between the timestamp of an Incident Ticket creation and effective restoration (workaround or definitive) of Sigfox Service(s) for the same Incident.
- **Communication frequency**: Elapsed time between each communication towards the entity reporting the incident and starting from the beginning of effective work on this incident

Timescales will differ depending upon:

- The priority level of the incident.
- Business Hours (BH) and Non Business Hours (NBH) as defined in the Channel Partner Agreement.

Incident Priority	Time to Log (internal)	Time To take into Account (TTAC)	Time To Solve	Communication Frequency
P1	<30 min	<30 min	< 4 hours	1 hour
P2	<30 min	<30 min	< 12 hours	4 hours
P3	NA	< 1 working Day	< 5 working days	N/A
Request	NA	< 1 working Day	< 30 working days	N/A

Table 2: Timescale of incident priority

The incident priority is set by the Channel when reporting the incident to Sigfox Operator's Service Desks. The incident level of Priority can be modified all along the process with Channel agreement.

21.3 Reporting an incident

The following information must be provided when reporting an incident:

- Incident summary
- Priority
- Incident start date/time
- Service impact
- Incident description

When logged, a unique identifier is associated to the incident and automatically communicated to the Channel.

Chapter 8
Channel Governance Plan

sigfox

22 Channel Governance Plan

22.1 Governance structure

Figure 59: Governance structure

- Strategic level:

The Steering Committee is composed by the Account managers and Service Managers from Sigfox and the Channel company. They define strategic orientation and represents the last level of escalation.

- Tactic level:

Monthly meeting/reporting to be held between Service managers from Sigfox and the Channel company. They are in charge of defining guidance as per strategic orientation; services are delivered in accordance 6 KPIs (main is SLA) and activities are performed according to contractual commitments and guidance.

- Operational level:

Service Desk is the main operational level. He is in charge of ensuring daily collaboration is efficient and applying the guidance.

22.2 Governance roles

The following table describes the different roles & their related responsibilities on the governance:

Distributor Roles	Responsibilities
Service Desk	Daily collaboration, the single point of contact for operational processes (Request for information, Incident, request for change).
Service Desk Manager	Escalate/blocked request to service manager, participate service manager meetings.
Channel Service Manager	Monthly meeting/ automatic reports, meeting on demand.
Account Manager	Strategy exchanges, last level of escalation, pricing evolution, major issues.

Table 3: Roles & responsibilities in the governance

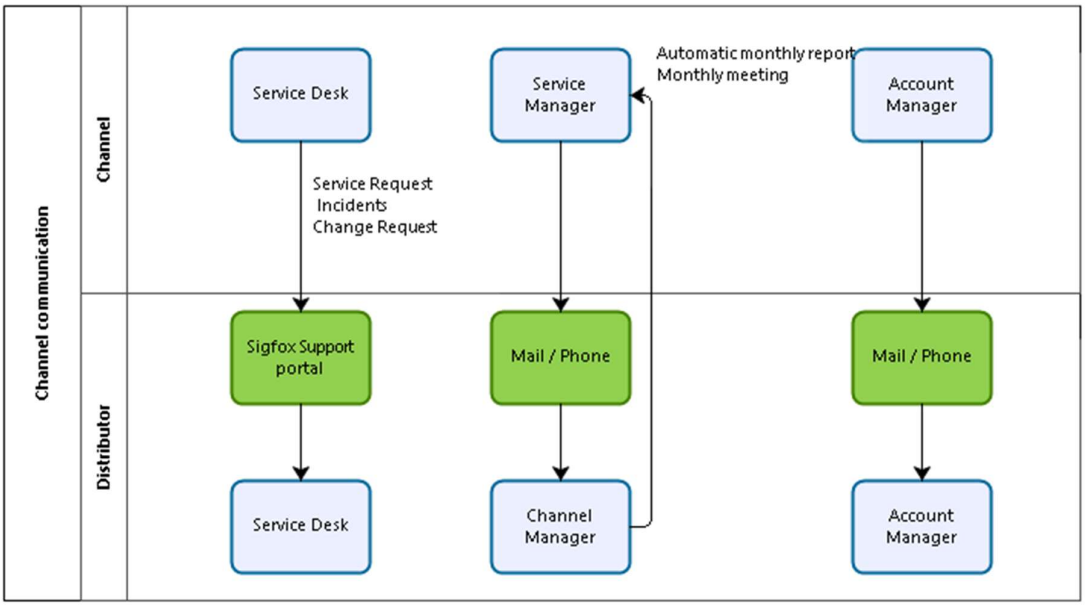


Figure 60: Channel communication path

22.3 Channel interface

After channel integration (device certified + IT integrated + specific network deployed), the channel is driven by Support team.

Two interfaces on Support team are defined:

- Technical assistance with Sigfox ticketing tool
- Contractual assistance with channel service manager and account manager contact

Depending of devices volume, channel will have two different channel service management:

- Volume < n devices: Automatic monthly report send by mail with meeting on demand (except stream meeting for specific subject). Maximum 1 for a year.
- Volume > n devices: Monthly meeting on Bluejeans with monthly report.

The Reporting format is the following:

- Maximum 1h/report for channel service manager.
- Maximum of 10 slides on report (1 page = 1 KPI).
- Minutes included after meeting.

22.4 KPIs overview

To feed these reports, Sigfox will provide all these following information. Some of basic information will be provided in project phase (like device geo-position).

List of identified KPIs :

- SLA device.
- SLO device.
- Base station statement (CaaS mode).
- Billing statement .
- Data analyse: example with erratic performance.
- Sigfox ticketing tool demands statistics?

List of acronyms

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
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
PAC	Portability authorisation code
SLA	Service level agreement
SLO	Service level objective
SO	Sigfox operator
SSL	Secure socket layer
TAP	Transfox access Point (BS)
TCO	Total cost of operation
UNB	Ultra-narrow band
VPN	Virtual private network