Sigfox Nano Access Point

(White paper)

Aug. 2021

Ver. 0.92

Copyright© 2021 All rights reserved by Remote Solution Co., Ltd.

TABLE OF CONTENTS

1 Introduction

Remote Solution will launch and distribute a new Sigfox basestation within its global markets. The new Nano access point is created to ensure increased coverage within blackspot areas in a cost-effective solution. This augments the choices by supporting different types of internet backhauls available to consumers and SMB customers.

The applications may also be extended via mobility functionality with GPS. As an example, International Transportation in cases of border crossing is supported via GPS and an “Automatic RC Change” feature. BLE and NFC are supported and those key features enable users to install and configure NAP much easier than before. It’s called “Zero touch installation”. A simple “Zero Touch” Installation feature that seamlessly connects homes to the Sigfox network.

The NAP product offers a new market segment and low-cost value proposition to customers considering or planning to upgrade the Sigfox service.

NAP has 3 different models categorized by their backhaul capability for internet connection. They are NAP3, NAP5 and NAP7. NAP3 supports Wi-Fi and Ethernet, NAP5 supports Cellular connectivity and NAP7 support both capability of NAP3 and NAP5 under the brand name “RS IoT”.

2 Acronyms and Abbreviations

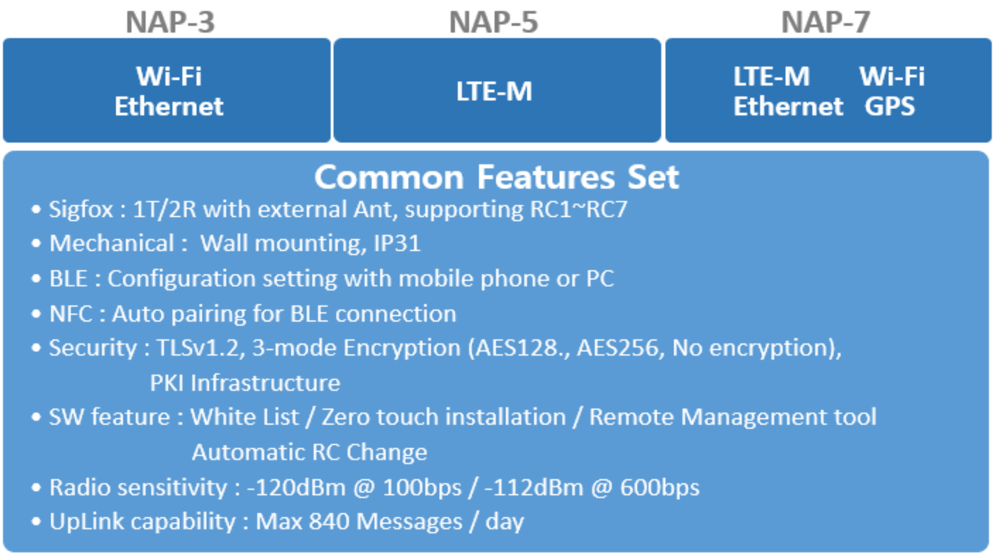
Items	Definitions
RS	Remotes Solution
BLE	Bluetooth Low Energy
NAP	Nano Access Point
RC	Radio Configuration
ZTI	Zero Touch Installation

[Table 1 Abbreviations]

3 Product Features

3.1 Product Specifications

NAP-3 supports Wi-Fi and Ethernet connection, NAP-5 supports LTE and NAP-7 supports LTE, Wi-Fi and Ethernet as a backhaul solution.



NAP-3: Wi-Fi, Ethernet

NAP-5: LTE-M

NAP-7: LTE-M, Wi-Fi, Ethernet, GPS

Common Features Set

- Sigfox : 1T/2R with external Ant, supporting RC1~RC7
- Mechanical : Wall mounting, IP31
- BLE : Configuration setting with mobile phone or PC
- NFC : Auto pairing for BLE connection
- Security : TLSv1.2, 3-mode Encryption (AES128., AES256, No encryption), PKI Infrastructure
- SW feature : White List / Zero touch installation / Remote Management tool Automatic RC Change
- Radio sensitivity : -120dBm @ 100bps / -112dBm @ 600bps
- UpLink capability : Max 840 Messages / day

[Figure 1   NAP Specification overview]

GPS function is a default feature on NAP-7, but it's optional on NAP-5. It supports IP31 for indoor installation as a default. For outdoor installation (IP65), outdoor enclosure can be utilized as an add-on feature. This can be provided by Remote Solution or users can purchase it in the market for user flexibility on IP65 choice.

There are 4 add-on features in NAP. They are PoE, Automotive Cigar Jack, GPS and outdoor enclosure. User can purchase them in the market or purchase them from Remote Solution as an accessary package. NAP supports the mobile or PC app for backhaul configuration via BLE and supports the auto BLE pairing via NFC as well. Security-wise, TLSv1.2 and AES128, ACE256 encryption are in ready and supports "white List" which is allowing NAP to receive message from the permitted devices.

NAP can give a value to save the installation time in Sigfox network via Zero touch Installation (ZTI). Installation data are pre-registered to Sigfox cloud during production. It helps to save registering time on installation.

NAP supports Remote Management system and Automatic RC change functions. Automatic RC change is for example, when NAP is crossing over the border, NAP changes its Radio configuration automatically for the new RC zone. It enables NAP to install on a truck or any vehicles for tracking their goods.

Radio sensitivity for Rx is -120dbm at 100bps and -112dbm at 600bps. Regarding uplink capability, NAP is able to receive 2 simultaneous uplink message and able to relay to Sigfox Cloud up to 840 messages per day.

NAP supports LTE, Wi-Fi, GPS(GNSS), BLE and NFC as a RF. These backhaul capability categorizes NAP to 3/5 and 7. Below table shows RF functionality of each models.

Model	LTE	Wi-Fi	GPS	BLE	NFC
NAP3		✓		✓	✓
NAP5	✓		✓	✓	✓
NAP7	✓	✓	✓	✓	✓

※ NAP5 support LTE as optional add-on function (Default NAP5 doesn't support LTE). NAP7 supports LTE as a default function.

3.2 ID Overview

Common IDE design for all models, with three configurations for varied use cases. The ID below indicates the NAP-7 model, which features two external antennas for LTE and Sigfox

Antenna variances

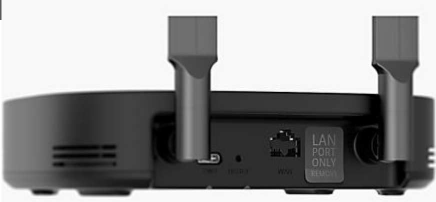
- 2 external antennas supported for LTE and Sigfox RF
- NAP3 has one antenna for Sigfox
- NAP5 and NAP7 have two antennas for LTE and sigfox
- External antennas are assembled on production. It's not allowed to detach from the body after launch. It helps t secure antennas and prevent antennas from theft in public.

LED Indicator variances

- 5 LEDs are supported in NAP (Power, Cloud Connection, LTE, Wi-Fi, Ethernet)

Model	Power	Cloud	LTE	Wi-Fi	Eth.
NAP3	✓	✓		✓	✓
NAP5	✓	✓	✓		
NAP7	✓	✓	✓	✓	✓

REAR Interfaces



- USB-C : Power Input
- Reset Switch (Recessed)
- Two RJ45 : One for WAN, The other for LAN

※ LAN Port is covered by a sticker on production

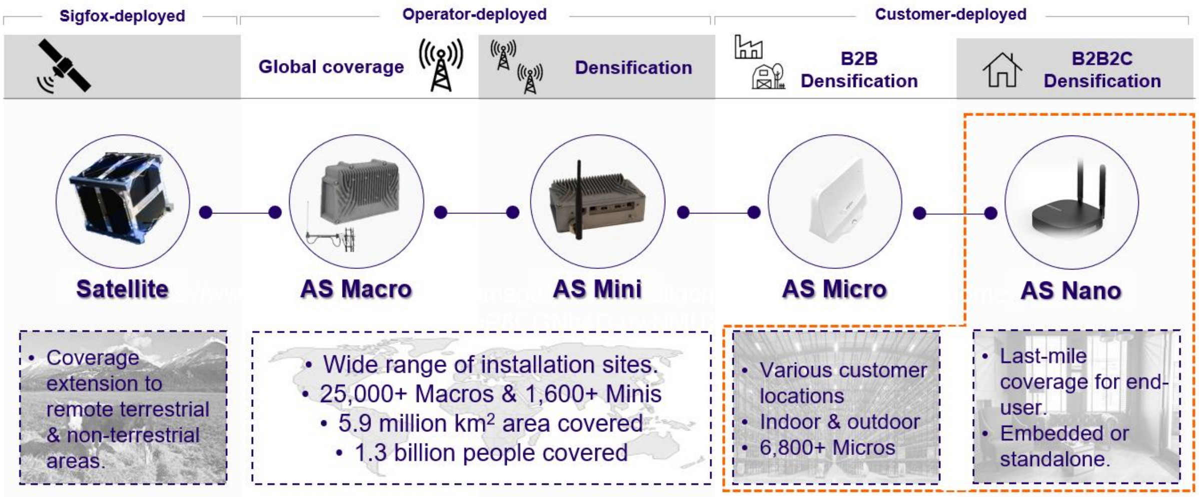
4 Benefits from NAP

4.1 Market extension to B2B2C or SMB via low-cost and multiple backhaul

Today, looking at Sigfox ecosystem, there are multiple types of base stations and they have composed of Sigfox networks and have been providing services to the customers.

Macro station covers a wide range of installation sites and it covers various customers' locations including indoor and outdoor. As of today, Macro and Micro stations are covering 5.9 million km^2 area and more than 1.3 billion people and in particular, Micro station is covering the various locations where Macro/Mini can't cover. Micro station is the smallest cell in the current Sigfox ecosystem and it helps Sigfox network can reach out to more closely to the last mile area.

Currently, there're many complexities on backhaul technologies in the last miles and market competitiveness is getting severe. This makes customers hesitate when they try to find out the best solution for where they live. It's because LPWAN IoT gateway doesn't catch up the speed of technology enhancement and diversity. Market wants much smaller devices and various functions to support this variety. In this regards, Micro station in last miles doesn't look like to fit in the customers' needs. This is more likely to target B2B market since its price range and capacity of coverage are positioned out of B2B2C market.


Sigfox-deployed
Operator-deployed
Customer-deployed
Global coverage
Densification
B2B
Densification
B2B2C
Densification
Satellite
AS Macro
AS Mini
AS Micro
AS Nano
• Coverage extension to remote terrestrial & non-terrestrial areas.
• Wide range of installation sites.
• 25,000+ Macros & 1,600+ Minis
• 5.9 million km² area covered
• 1.3 billion people covered
• Various customer locations
• Indoor & outdoor
• 6,800+ Micros
• Last-mile coverage for end-user.
• Embedded or standalone.

[Figure Nano Positioning – within the Sigfox Network solutions]

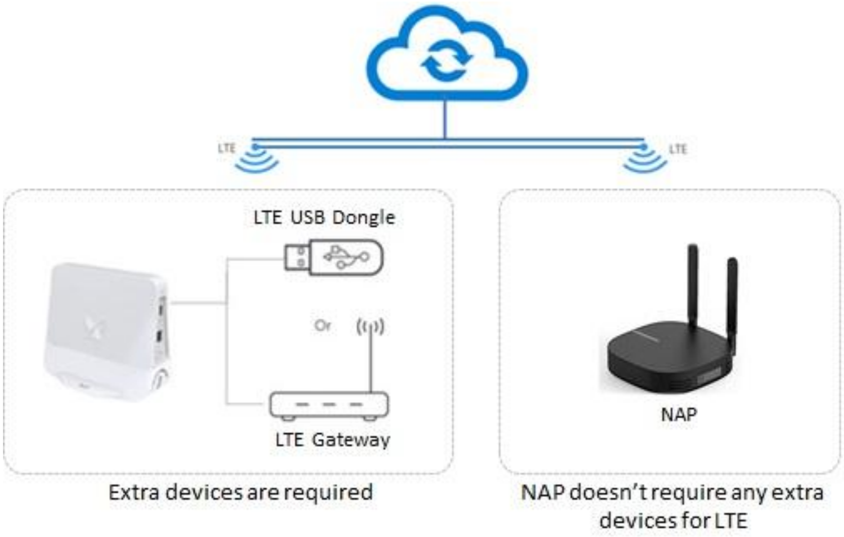
With this background, NAP is going to debut in the market Q2, 2022.

NAP has multiple backhauls capability for the diverse environment in the last mile. It supports Ethernet, Wi-Fi, and LTE as the internet connection. This helps to decrease the dependency on a choice of internet connectivity where they live.

For instance, let's assume there is a person who runs a small or medium size of grocery store. Every day, he has to receive fresh food from their supplier and he needs to keep them at a constant temperature because it easily goes bad. In order to sort out this, he probably needs some services in a smart way with a minimum effort. Like the other SMB, he subscribes to internet service and needs to have a router making a Wi-Fi coverage in his store.

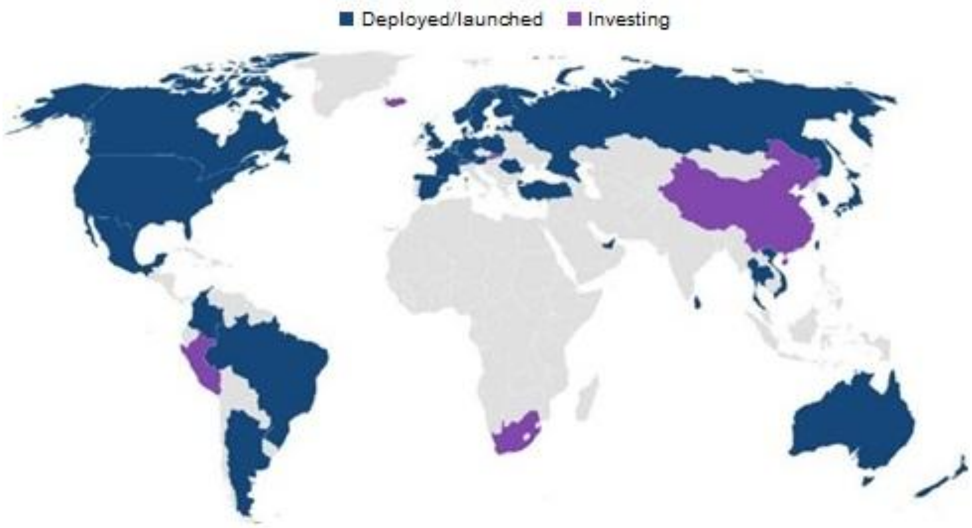
NAP is the best solution in this environment. It gathers temperature information sent by IoT things on a refrigerator or in a food warehouse and sends them to Sigfox Cloud by Wi-Fi backhaul. For LTE users who want to use LTE instead of subscribing to internet service, NAP provides LTE backhaul without additional devices such as LTE dongle or LTE router.

Comparing to a previous model Micro, this doesn't require LTE receiver such as an LTE dongle or an LTE router (or LTE gateway) and it doesn't bring the customers a new cost burden.


LTE
LTE
LTE USB Dongle
Or
LTE Gateway
NAP
Extra devices are required
NAP doesn't require any extra devices for LTE

NAP supports diverse LTE capabilities. Default LTE capability in NAP is LTE-M1 which is enhanced Machine Type Communication. It's a type of lower power wide area network(LPWAN) radio technology standard which enables a wide range of cellular devices and services.

In March 2019, the Global Mobile Suppliers Association reported that over 100 operators had deployed and launched LTE-M network.



In order to meet requirements for a wider range of IoT use cases and to satisfy coverage LTE in NAP, LTE Cat1 is applied to NAP as its LTE variance. Depending on the region where NAP is required, LTE Ca1 and LTE M1 are an optional feature that allows customers to select it.

Specification	Cat 1 (optional)	M1 (default)
Total Bandwidth Required	20Mhz	1.4Mhz
Download Peak Rate	10 Mbps	1 Mbps or 375Kbps
Upload Peak Rate	5Mbps	1 Mbps or 375Kbps
Power demand	Low	Very low
Duplex mode	Full duplex	Full duplex or half duplex

From a cost perspective, NAP brings extra benefits to the customers. Comparing the unit price between NAP and Micro station, the unit price of NAP is much lower than Micro, which enables SOs to save costs simply by replacing Micro with NAP in a low-density area.

NAP provides a more efficient way of the installation which is called "Zero touch installation" and enhanced configuration tools by mobile applications. It helps to save installation time and its efforts.

Providing those new features, NAP offers a new market segment and low-cost value proposition to customers in Sigfox ecosystem.

4.2 Moving Asset Tracking via GPS functionality

Various industries are now adopting advanced IoT technologies to bring improvement in range of different areas.

One such area is asset tracking. GPS tracking technologies have been around for a long time and now with all the innovations in the areas of sensors, networking, and connectivity, the technology is well-suited as well as cost-effective to track assets and vehicles in real-time for commercial and industrial applications.

The transportation industry has been the largest user of GPS tracking solutions. Although long-haul fleet carriers represent one of the largest segments, there has been growth in tracking solution sales to various other asset-intensive industries such as automotive, aerospace & defense, mining, and oil & gas. These industries are adopting asset-tracking technologies for tracking and monitoring asset location and statuses to get more visibility into their asset utilization.

Industries are also realizing that they can leverage tracking technologies to better manage their assets and to significantly improve asset performance.

Asset tracking technologies offer range of benefits. Some key benefits are listed below:

1) Real-time Location Tracking

With exact GPS co-ordinate information, maintenance personnel can easily locate an asset.

GPS tracking technologies also help managers access real-time asset status information, as well as historical location and status data. This helps them better understand how their operations are running, and find areas where efficiency can be improved.

2) Geofencing

A geo-fence is a virtual barrier surrounding real-world geography. With GPS tracking technology, users can set up a virtual boundary for their assets.

Whenever an asset goes out of this boundary, they receive an alert or notification. Setting virtual boundaries via geofencing can be extremely helpful for asset managers.

First, it ensures that asset is safe and helps avoid theft. Second, it ensures safety. Industries such as mining and oil & gas are by nature hazardous. It is not uncommon for these industries to have restricted areas, where extreme caution needs to be exercised to enter such areas. In case, any vehicle enters these areas by mistake, manager gets instant alert and can respond quickly.

3) Asset Usage Data

The location data collected with the help of GPS trackers can help managers get better insight on various usage parameters, such as mileage and fuel consumption. By having a better understanding of these parameters, managers can easily evaluate inefficiencies in the transportation process. They may identify assets that are not energy-efficient or wasting fuel with excessive idle time, or not taking optimal routes. End-users can also integrate their tracking data with their other asset management systems for added visibility and better planning.

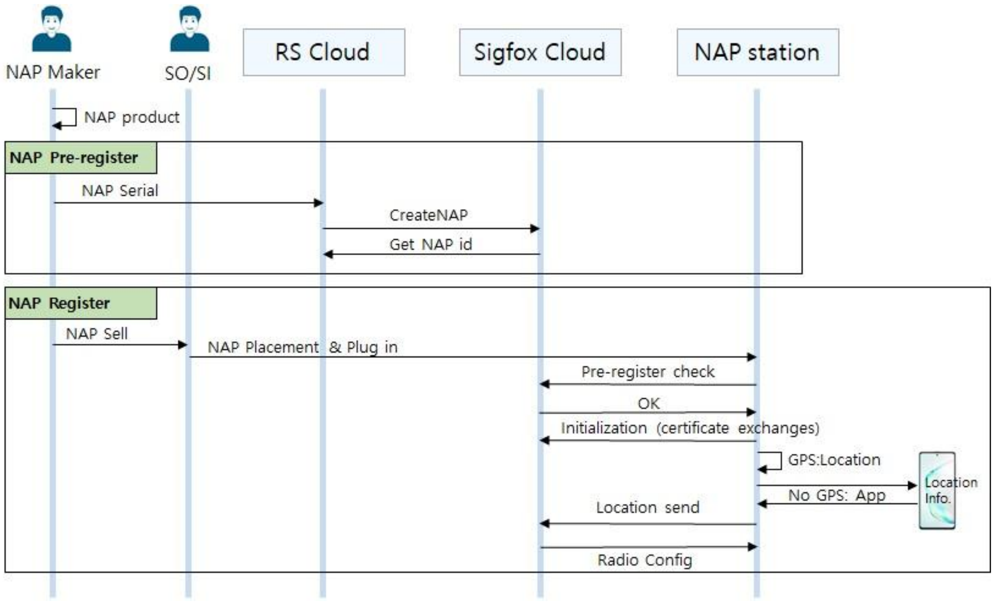
4.3 Easy Installation via ZTI and Mobile App

NAP provides ZTI (zero Touch Installation) service through a pre-registration process of maker.

ZTI provides a Mobile App that can acquire location information of Mobile in order to acquire location information, which is mandatory registration information.

When a user plugs in, Sigfox Cloud recognizes the NAP that has been plugged in and performs the automated installation process to register the NAP.

The automatic registration process is as follows.



When NAP is sold, Remote solution registers the NAP information in SigFox Cloud before supplying the NAP.Therefore when the installer plugs in NAP, the registration process is performed automatically.

Location information required for service must be entered at the registration stage.

In case of a NAP with a GPS module, the location information is obtained from the GPS module and the location of the NAP is registered.

If the NAP is not equipped with a GPS module, the location information is registered by recognizing the location information of the Mobile App through NFC pairing between the NAP and the mobile phone.

4.4 Private Network via White List functionality

A whitelist (or, less commonly, a passlist or allowlist) is a mechanism which explicitly allows some identified entities to access a particular privilege, service, mobility, or recognition i.e. it is a list of things allowed when everything is denied by default. It is the opposite of a blacklist which is list of things denied when everything is allowed by default.

What Is Whitelisting?

Whitelisting involves only allowing access for **approved entities.**

The default is to **block access.**

Whitelisting is **trust-centric.**

- **When to use whitelisting**

If you want to maximize security and don’t mind the extra administrative effort or limited accessibility, whitelisting is the best choice. Whitelisting is ideal when stringent access control and security are crucial.

Whitelisting works well for systems that aren't public. If you have an application that only select employees of your company need access to, for example, you could whitelist the IP addresses of their computers and block all other IP addresses from accessing the app.

Additionally, whitelisting can be useful when you want to define what actions an application or service can perform and restrict it from doing anything else. You can accomplish this by whitelisting certain types of behavior.

Use whitelisting when:

- Only a select group of users needs to use a system.
- You want a more controlled environment.
- You don't mind investing more administrative effort.

In our case, Whitelisting is when you grant network (NAP) access only to specific sigfox ID (sigfox device).

Whitelist is essential for Private network and good to have for security strategy.

Customer can tailor-make whitelists based on their unique wants and needs.

4.5 Easy Remote management via Remote management System

RMS(Remote management Service) provides the ability to remotely NAP settings, change the status, and monitoring

This function provides not only the Web but also the Mobile App service, and provides various functions for the customer's IoT service.

The main features provided by RMS are:

- **Register and Read NAP**

  When the installer plugs in NAP, it can automatically perform the registration process and query the NAP information.

  When NAP is installed for the first time or additionally for service expansion, convenient registration helps quick installation and helps you to check service status by inquiring NAP information at any time.

- **NAP status control**

  The status of NAP can be adjusted to Mute, Deactivate, Disable, etc. depending on the N/W or service status.

  This processing can be remotely coordinated according to regulations set by SigFox and can be utilized as appropriate depending on the status of the service and NAP.

- **RFM (Remote Firmware Management)**

  RFM can remotely upgrade F/W to NAP performance improvement or improve errors.

  RFM can add necessary functions to F/W for improved service.

- **Whitelisting**

  If you configure private service, NAP can only provide services to allowed end devices.

  NAP restricts the service for disallowed end devices and supports the configuration of stable private services.

- **Tracking support (2nd Phase)**

  If you configure a private service using NAP, RS cloud can provide a tracking function for the end device.

  The service is based on GIS and RS will be able to provide customized tracking services that customers want.

- **RMS services will be added step by step.**

4.6 Prevention from hacking via powerful security features

4.6.1 Security by Design

- **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.

⇨ Authentication. Each Sigfox Ready™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.

⇨ Anti-replay. Each Sigfox message contains a sequence counter which is verified by the Sigfox Core Network to detect and discard replay attempts. The integrity of the counter is guaranteed by the message authentication token.

⇨ Anti-eavesdropping. 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.

- **Security of data at rest**

Critical data is stored in all entities of the IoT chain.

⇨ Sigfox Ready™devices store their authentication key.

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 Ready™ 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 Ready™ devices' authentication keys as well as traffic metadata. State-of-the-art solutions have been deployed to ensure the integrity, availability and confidentiality of these data. A continuous improvement process has been defined to ensure that Sigfox Core Network is compliant with local regulations.

4.6.2 Reliability & Reliance

Reliability and reliance of the IoT applications requires high availability of the Sigfox network and resistance to attacks.

Sigfox approaches this aspect in both the radio and the IT segments.

In the radio segment, a high level of redundancy is provided by the non-connected nature of the Sigfox Radio Access layer in which Sigfox ReadyTM devices broadcast their messages, and all base stations in their range receive and relay the message to the core network. This mode of operation also protects against some forms of malicious jamming attempts.

Moreover, since the Sigfox Core Network acts as a firewall, it has the opportunity to monitor and detect traffic anomalies and block traffic from selected base stations, or selected customer applications when attacks are suspected. This efficiently reduces the scope and impact of DoS attacks based on the radio segment targeting access points or the Sigfox network, and practically rules out Sigfox ReadyTM devices as DDoS attack vectors.

In the IT segment, the Sigfox Core Network is essentially a cloud-based network. As such, it benefits from proven internet technologies and suppliers.

More specifically, the Sigfox Core Network is hosted in secured certified data centers. Each rack is secured2 with biometric protection for physical access.

Each data center is doubly internet-attached through different internet transit providers. By design, Sigfox architecture is fully load-balanced and redounded from the core switching to the applicative servers based on virtual machines through double-attached physical servers. At the application layer, each component is fully redundant, strongly monitored and fully scalable to support any increase in traffic.

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

A dedicated solution protects Sigfox data centers against a wide range of denial-of-service cyber-attacks such as denial-of-service (DoS), distributed denial-of-service (DDoS), reflective denial-of-service (RDoS), and distributed reflective denial-of-service (DRDoS). This solution, supplied and maintained by our internet service provider, offers a cloud-based protection service with several scrubbing centers in order to detect and mitigate cyber-attacks against networks and websites. This solution uses proprietary detection and mitigation algorithms matching Sigfox-specific traffic patterns to prevent false positives.