Sigfox overview

Sigfox

Version 1.0

Hello, and welcome to this presentation of the Sigfox protocol.

Sigfox overview

- Sigfox is using free Unlicensed spectrum below 1GHz
- Ultra Narrow Band
  - Signal transmitted by a Sigfox object requires only 100Hz of Band (600Hz for FCC regions)
- Bi-directional
- Half Duplex (Tx then Rx)
- Small messages up to 12 bytes
- Max 144 messages per day
- Large Link Budget 140dB => Range >10kms

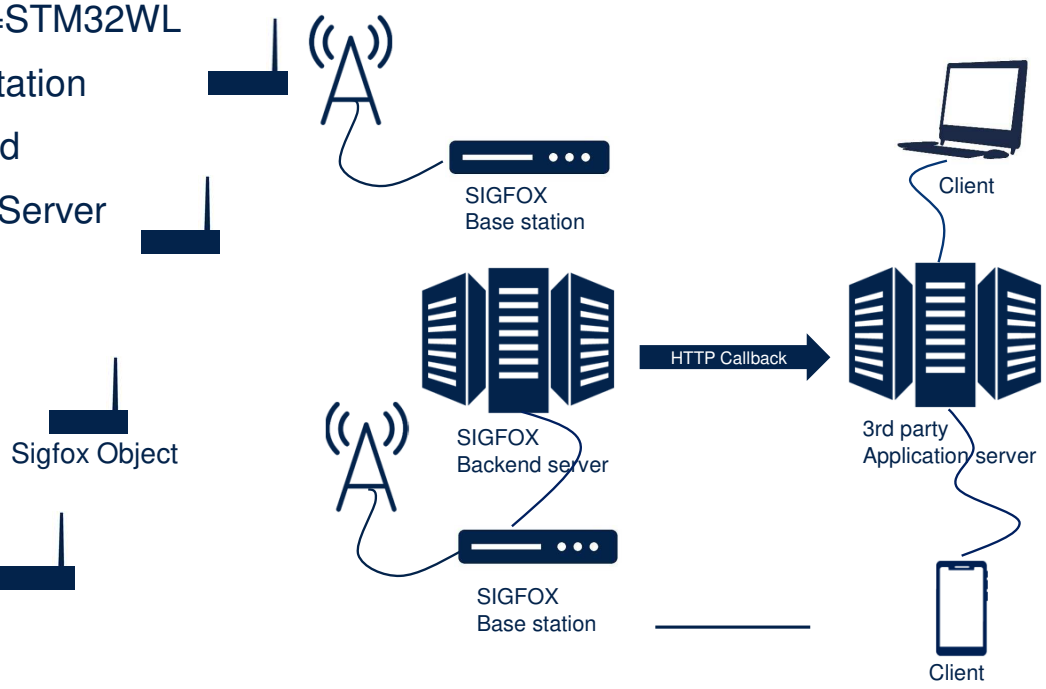
life.augmented

Sigfox is using the free Unlicensed spectrum below 1GHz
It uses an Ultra Narrow Band: The signal transmitted by a Sigfox object requires only 100Hz of Band (600Hz for FCC regions)
Its main characteristics are:

- Bi-directional
- Half Duplex (Tx then Rx)
- It can deliver small messages up to 12 bytes with a maximum of 144 messages per day
- With a Large Link Budget of 140dB , the achievable range is over 10kms.

Network architecture

- Sigfox Object=STM32WL
- Sigfox Base Station
- Sigfox Backend
- 3rd Party App Server

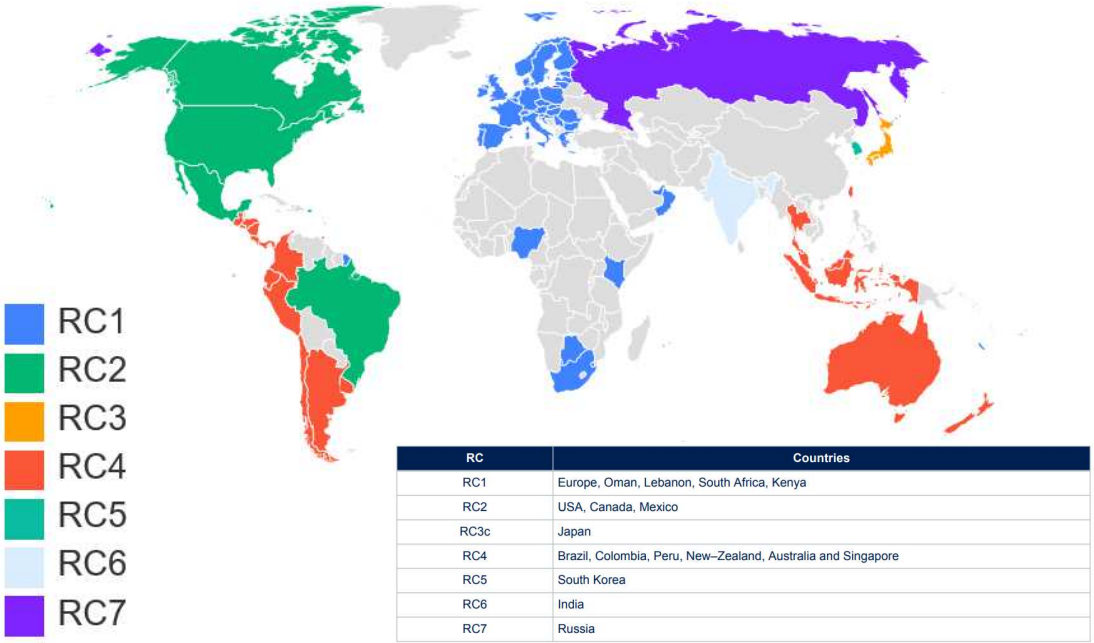


life.augmented

3

The network architecture is shown in this picture: Sigfox IoT objects which may run on battery are wirelessly connected to a the Sigfox Network. Sigfox Network is composed of Sigfox Base Station relaying messages to the Sigfox Back-End Server. Messages are forwarded to 3rd party application server that may be used to manage a fleet of devices.

Region configuration overview



RC	Countries
RC1	Europe, Oman, Lebanon, South Africa, Kenya
RC2	USA, Canada, Mexico
RC3c	Japan
RC4	Brazil, Colombia, Peru, New–Zealand, Australia and Singapore
RC5	South Korea
RC6	India
RC7	Russia

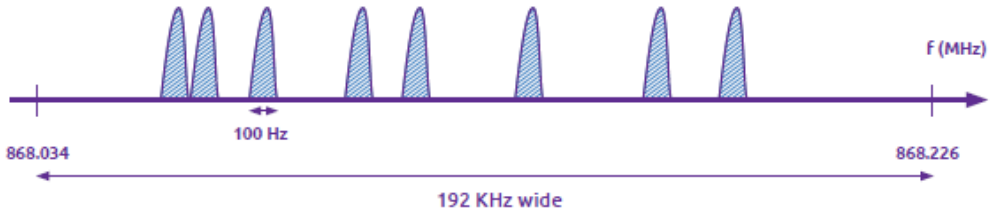
life.augmented

4

The European, North American and Asian markets have different spectrum allocations and regulatory requirements. Sigfox has split requirements in various region configurations called RC.
7 Regions Configurations are available and are depicted in this picture.

Ultra narrow band (UNB)

- In Europe, the frequency band ranges from 868 to 868.2 MHz;
- In the rest of the world, the band ranges from 902 to 928 MHz with restrictions according to local regulations.



life.augmented

Sigfox uses Ultra Narrow band modulated signals to send information to the Sigfox network enabling many devices to send data concurrently to the Sigfox network. Sigfox is using 192KHz of the publicly available band to exchange messages over the air. Each message is 100 Hz wide and transferred with a data rate of 100 bits per second, or 600Hz wide with data rate of 600Hz depending on the region.

RF specification

RF parameter	RC1	RC2	RC3c	RC4	RC5	RC6	RC7
Frequency band downlink (MHz)	869.525	905.2	922.2	922.3	922.3	866.3	869.1
Frequency band uplink (MHz)	868.130	902.2	923.2	920,8	923.3	865.2	868.8
Uplink modulation	DBPSK						
Downlink modulation	GFSK						
Uplink data-rate	100	600	100	600	100	100	100
Down-link data-rate	600						
Max output power (dBm)	14	22	13	22	13	13	14
Medium access	Duty cycle 1%	Frequency hopping Max on time 400 ms/20 s	Carrier sense	Frequency hopping Max on time 400 ms/20 s	Carrier sense	uty cycle 1%	
CS center frequency (MHz)	NA		923.2	NA	923.3	NA	
CS bandwidth (kHz)			200	NA	200		
CS threshold (dBm)			-80	NA	-65		

* Duty cycle is 1% of the time per hour. For an 8 to 12 bytes payload, this means 6 messages per hour leading to 140 messages per day

** Frequency hopping: The device broadcasts each message 3 times on 3 different frequencies. Maximum on time 400 ms per channel. No new emission before 20s.

*** Listen Before Talk: Devices must verify that the Sigfox-operated 200KHz channel is free of any signal stronger than -80dBm during 5ms before transmitting. When the channel is free, the device starts a transmission. The transmission is not started otherwise.

life.augmented

6

Sigfox RF specifications for medium access are depicted in this table. Frequencies, data rates, output power and medium access depend on the region where the device is operating.

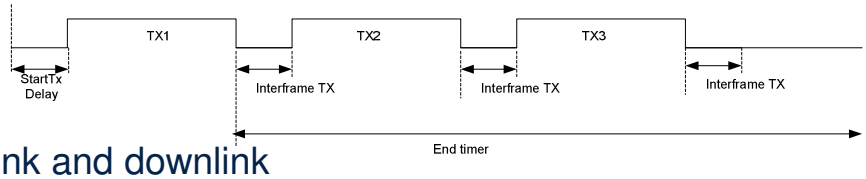
3 main groups of RF specifications can be highlighted which feature same data rates, e.g Duty Cycle (regions RC1, RC6 and RC7), Frequency Hopping (regions RC2 and RC4) and LBT (regions RC3 and RC5).

- Duty cycle is 1% of the time per hour. For an 8 to 12 bytes payload, this means 6 messages per hour leading to 140 messages per day
- Regarding frequency hopping, the device broadcasts each message 3 times on 3 different frequencies. Maximum on time 400 ms per channel. No new emission before 20s.
- Listen Before Talk (LBT): Devices must verify that the Sigfox-operated 200KHz channel is free of any signal stronger than -80dBm during 5ms before transmitting.

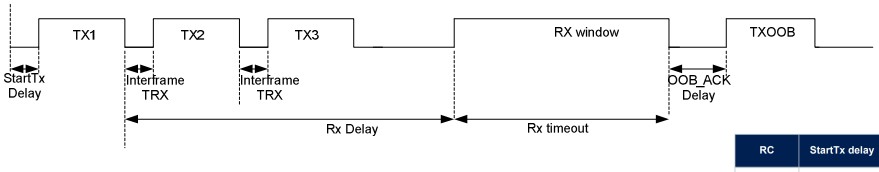
When the channel is free, the device starts a transmission. The transmission is not started otherwise.

Sigfox frame timings

- Uplink frame Only



- Uplink and downlink



RC	StartTx delay	Interframe Tx/TRx	Rx delay	Rx timeout	OOB_ACK delay	End timeout
RC1	0 s	500 ms	20 s	25 s	1.4 s	NA
RC2						10 s
RC3c	100 ms max (start LBT)	500 ms + LBT	19 s	34 s		NA
RC4	10 s	500 ms	20 s	25 s		
RC5	100 ms max (LBT)	500 ms + LBT	19 s	34 s		
RC6	0 s	500 ms	20 s	25 s		
RC7						

life.augmented

7

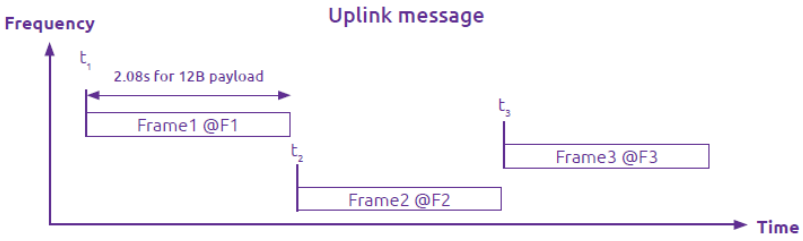
The end device transmits data to the network in an asynchronous manner as transmission data is only sent per device-report event. The figures below depict the timing sequences with and
without a downlink.
The three transmissions Tx1, Tx2 and Tx3 contain the same payload information. These consecutive transmissions only maximize the probability of a correct reception by the network. When the device observes a good link quality to the network, it may decide to send only Tx1 to save power consumption only if downlink frame is requested.
Note that Tx periods depend on the number of bytes sent and on the RC zone:

- It takes 10 ms to send a bit in RC1 and RC3c.
- It takes 1.66 ms to send a bit in RC2 and RC4.

A message can be 26-byte long at the most (including sync word, header, and payload data). Therefore, for RC1, a Tx period can be maximum 26 x 8 x 10 ms = 2.08 s.

Frequency hopping

- The device transmits a message on a random frequency and then sends 2 replicas on different frequencies and time slots.



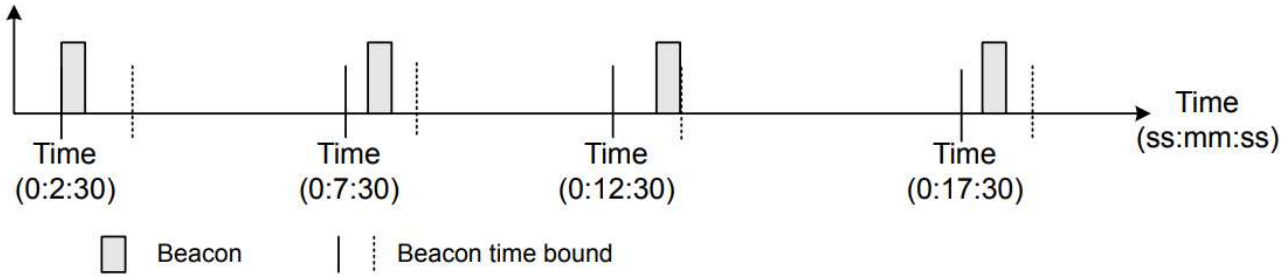
- The Sigfox base stations monitor the full 192 kHz spectrum and look for any UNB signals to demodulate at any time and any frequency

life.augmented

8

The device transmits a message on a random frequency and then sends 2 replicas on different frequencies and time slots. The Sigfox base stations monitor the full 192 kHz spectrum and look for any Ultra Narrow Band (UNB)signals to demodulate at any time and any frequency.

Sigfox Monarch



- Sigfox Monarch service is a Sigfox global service allowing to determine the zone where a device is located.
- The Monarch feature allows a Sigfox IoT device to roam seamlessly across the world.
- Monarch is a Sigfox beacon emitted from point of interest (POI).

life.augmented

Monarch is a Sigfox beacon emitted from a point of interest (POI). The Monarch beacon is emitted at a frequency allowed by the region the POI belongs to. The beacon contains region configuration (RC) information that a Monarch-capable device can demodulate. Upon reception of this information, the Monarch-capable device is able to switch automatically to the right Region Configuration and can send information to the network. The Monarch feature allows a Sigfox IoT device to roam seamlessly across the world.

The Monarch signal is sent at POI every 5 minutes plus a random back-off period of 10 seconds. The frequency of the beacon is region specific. The beacon lasts in total 400 ms. If a device clock is set, it is hence possible to open a scan window only when the Monarch signal is present to reduce current consumption of the end device.

Sigfox security

- The Sigfox ecosystem integrates the security by-default:
  - authentication & integrity
  - anti-replay on messages propagated on the network (sequence number)
  - cryptography based on Advanced Encryption Standard (AES) with no key over the air transmission
  - payload encryption as an option to ensure the confidentiality of the data
- Three different levels of security.
  - medium level – the security credentials are stored in the device;
  - high level – the security credentials are stored in a S/W based protected area, using the key management system (KMS);
  - very high level – the security credentials can be stored in a secure element.

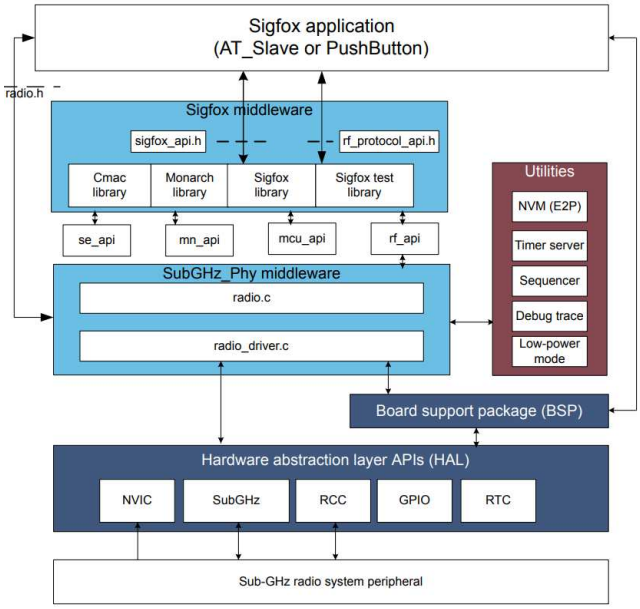
life.augmented

The Sigfox ecosystem integrates the security by-default:
- authentication & integrity
- anti-replay on messages propagated on the network (sequence number)
- cryptography based on Advanced Encryption Standard (AES) with no key over the air transmission
- payload encryption as an option to ensure the confidentiality of the data

There are three different levels of security.
- medium level – the security credentials are stored in the device;
- high level – the security credentials are stored in a S/W based protected area, using the key management system (KMS);
- very high level – the security credentials can be stored in a secure element.

Single Core STM32WL FW

- Sigfox application examples
- Sigfox stack middleware
  - Sigfox ™ MAC layer including Monarch
  - Sigfox Crypto driving a secure element or SKS
- SubGHz_Phy middleware
- Utilities
  - Timer Server
  - Low Power Management
  - Debug Trace
  - Emulated Eeprom
- HAL drivers
- BSP External component RF driver



life.augmented

11

2 types of Sigfox applications are provided in the STM32CubeWL Firmware Package. Both applications are available for single core devices and dual core devices. Only Single Core Sigfox application architecture is depicted here.
The HAL uses STM32Cube APIs to drive the hardware required by the application.
The RTC provides a centralized time unit that continues to run even in the low-power Stop mode.
The RTC alarm is used to wake up the system at specific times managed by the timer server.
The Sigfox Core library embeds the medium access controller (MAC) as well as some security functions.
The application is built around an infinite loop including a scheduler. The scheduler processes tasks and events. When nothing remains to be done, the scheduler transitions to idle state and calls the low-power manager.

Test mode and certification

- Any Sigfox device must pass the Sigfox certification to communicate on the Sigfox Network
  - Sigfox delivers Sigfox Verified™ certificate to acknowledge compliance to Sigfox RF & protocol specifications of a Modular Design and Development solutions.
  - Sigfox Ready™ certification is mandatory for any Device to be connected to the Sigfox network. A Device candidate for Sigfox Ready™ certification must comply to all Sigfox Certification Specifications (Sigfox RF & protocol and Sigfox radiated performance).
  - More info can be found under https://build.sigfox.com/certification
  - **The system including the NUCLEO-WL55JC board and the STM32CubeWL firmware modem application has been verified by Sigfox Test Lab and passed the Sigfox Verified™ certification**
- All Test modes are accessible via AT commands
  - Test modes can be checked in front of RSA SDR dongle tester
    - Note that sensitivity can not be tested with this tester

life.augmented

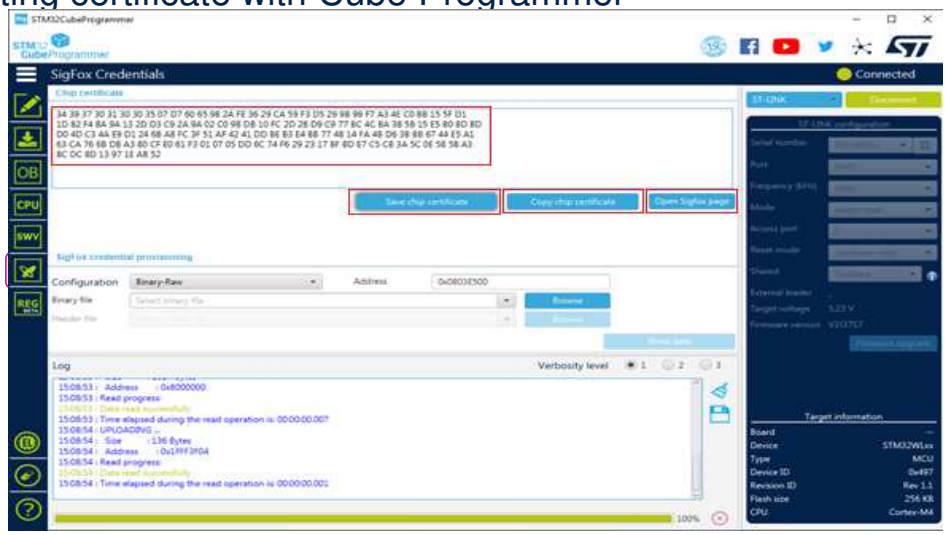
12

Any Sigfox device must pass the Sigfox certification to communicate on the Sigfox Network.
Sigfox delivers Sigfox VerifiedTM certificate to acknowledge compliance to Sigfox RF & protocol specifications of a Modular Design and Development solutions.
Sigfox ReadyTM certification is mandatory for any Device to be connected to the Sigfox network. A Device candidate for Sigfox ReadyTM certification must comply to all Sigfox Certification Specifications (Sigfox RF & protocol and Sigfox radiated performance).
More info can be found under https://build.sigfox.com/certification
The system including the NUCLEO-WL55JC board and the STM32CubeWL firmware modem application has been verified by Sigfox Test Lab and passed the Sigfox VerifiedTM certification
All Test modes are accessible via AT commands.

How to make communication with Sigfox Network (1/4)

1- Compile and load Sigfox_AT_Slave project

2- Getting certificate with Cube Programmer



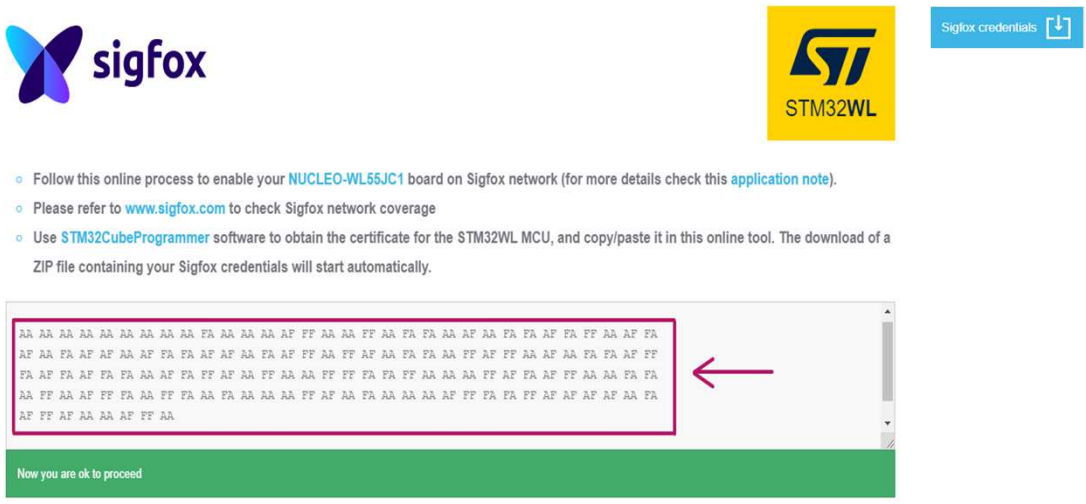
life.augmented

13

The coming slides describe the successive steps to make a communication with the Sigfox network.
First compile and load Sigfox_AT_Slave project from STM32CubeWL Firmware Package.
Then starts the STM32CubeProgrammer and connect to the STM32WL. A button labeled Sigfox Credentials is added on the main menu on the left end-side.
After opening the Sigfox Credentials window, the chip certificate is extracted automatically with 136-byte size and displayed in chip certificate area. This certificate can be saved in a binary file and copied to the clipboard.

How to make communication with Sigfox Network (2/4)

3- copy/past credentials on https://my.st.com/sfxp, and download the credentials

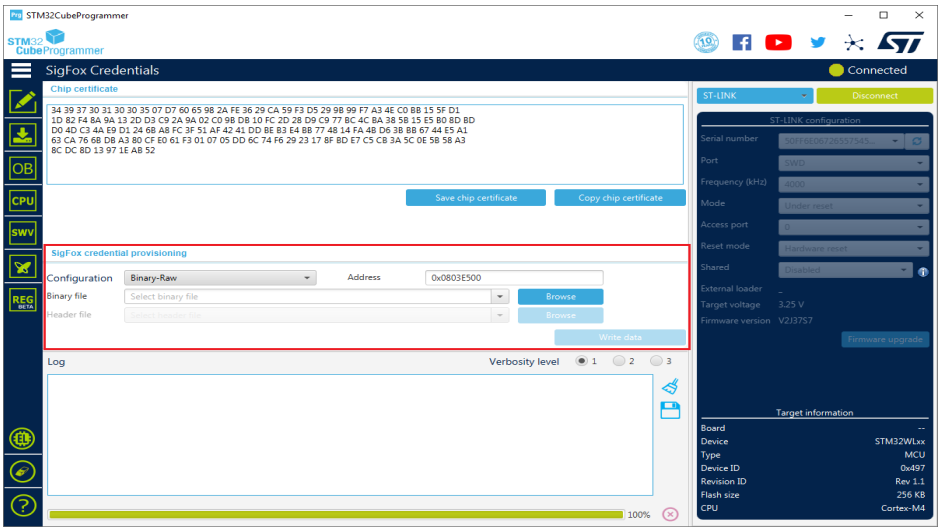


life.augmented

ST provides a web interface on my.st.com, where the user can get the Sigfox trial credentials.
Go to https://my.st.com/sfxp and register on my.st.com to create a specific user account (if not yet done).
Then paste the certificate extracted with STM32CubeProgrammer into the form.
If the Certificate is valid, click on the download button and the zip file is automatically downloaded on the user computer.

How to make communication with Sigfox Network (3/4)

- 4- Load Credentials in STM32WL



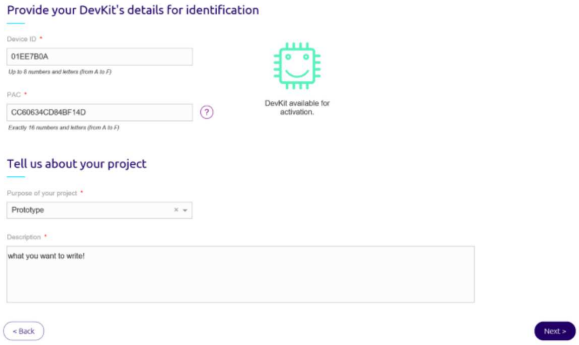
life.augmented

15

Once un-zipped, the credentials can be loaded in the STM32WL device, using the Sigfox credential provisioning area in the STM32CubeProgrammer.

How to make communication with Sigfox Network (4/4)

- 5- Activation https://buy.sigfox.com/activate/
  - Use AT$ID? and AT$PAC? commands on your preferred terminal to get Sigfox ID and PAC.



  - Click next. Your device is ready to send data to Sigfox™ network
    - Go to https://backend.sigfox.com/device/list to see the device listed (click on DEVICE). Data can be sent using the AT$SF command on the terminal

life.augmented

16

Use AT$ID? and AT$PAC? commands to get Sigfox ID and Sigfox PAC.
Login on https://buy.sigfox.com/activate/ and paste the device ID and PAC into the activate
and click Next, and the device will be activated.
To see the message, log on https://backend.sigfox.com/ and browse to the device list where the device should be visible.
Data can be sent using the AT$SF command on the terminal. The device sends data to the Sigfox network and messages are visible on the backend (click on the device ID and the go on the MESSAGES tab).

Resources

- More information can be found in AN5480
  - How to build a Sigfox™ application with STM32CubeWL

life.augmented

More information can be found in AN5480 regarding the way to build a Sigfox™ application with STM32CubeWL.