

Beanair GmbH

DOCUMENT			
Document ID	TN_RF-021	Version	V1.0
External reference	TN_RF-021	Date	30/03/2020
Author	Achref CHAABENI, Test & validation Engineer		
		Project Code	
Document's name	TN-RF-021-SSL-TLS-Encryption-MC	QTT	

	VALIDATION		
Fonction	Destination	For validation	For info
Writer		✓	
Reader		✓	
Validation			√

DIFFUSION			
Fonction	Destination	For action	For info
Reader n°1	Antje Jacob, Production Manager	✓	
Reader n°2	Omar SKANDER, Embedded software engineer	~	

UPDATES			
Version	Date	Auteur	Evolution & Status
1.0	30/03/2020	Achref CHAABENI	First version of the document

# Disclaimer

The contents are confidential and any disclosure to persons other than the officers, employees, agents or subcontractors of the owner or licensee of this document, without the prior written consent of Beanair GmbH, is strictly prohibited.

Beanair makes every effort to ensure the quality of the information it makes available. Notwithstanding the foregoing, Beanair does not make any warranty as to the information contained herein, and does not accept any liability for any injury, loss or damage of any kind incurred by use of or reliance upon the information.

Beanair disclaims any and all responsibility for the application of the devices characterized in this document, and notes that the application of the device must comply with the safety standards of the applicable country, and where applicable, with the relevant wiring rules.

Beanair reserves the right to make modifications, additions and deletions to this document due to typographical errors, inaccurate information, or improvements to programs and/or equipment at any time and without notice.

Such changes will, nevertheless be incorporated into new editions of this document.

Copyright: Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights are reserved.

Copyright © Beanair GmbH 2020

# Contents

1.	TECI	TECHNICAL SUPPORT		
2.	VISU	JAL SYMBOLS DEFINITION	8	
3.	ACR	ONYMS AND ABBREVIATIONS	9	
4.	DOC	CUMENT ORGANIZATION	. 10	
5.	MQ	TT CONFIGURATION	. 11	
	5.1	Broker	. 12	
	5.2	Keep alive	. 12	
	5.3	Authentification	. 13	
	5.4	SSL/TLS	. 13	
	5.5	CERTIF	. 14	
	5.6	MQTT STATUS	. 14	
	5.7	Topic for static measurement	. 15	
	5.8	topic for Dynamic measurement	. 15	
	5.9	Subscribe	. 16	
6.	SSL	CONFIGURATION	. 17	
	6.1	Introduction about SSL	. 17	
	6.2	SSL encryption for MQTT communication	. 17	
	6.3	SSL for OtaOp communication	. 20	
	6.4	SSL for Beanscape <sup>®</sup> Wilow <sup>®</sup>	. 21	
	6.5	Example of MQTT Broker on teltonika router (rut240/rut950)	. 21	

# **List of Tables**

No table of figures entries found.

# **List of Figures**

Figure 1: BeanDevice <sup>®</sup> Wilow <sup>®</sup> menu	11
Figure 2: MQTT Module window	11
Figure 3: Broker frame	12
Figure 4: Keep alive frame	12
Figure 5: Authentication frame	13
Figure 6 SSL/TLS	13
Figure 7 Certif	14
Figure 8: MQTT Status frame	14
Figure 9: Topic for static measurement frame	15
Figure 10: Topic for dynamic measurement frame	15
Figure 11: Subscribe	16
Figure 12 OpenSSL command	17
Figure 13 SSL/TLS configuration	18
Figure 14 MQTT configuration	19
Figure 15 MQTT configuration window	19
Figure 16 firmware uploader	20
Figure 17 MQTT Broker	22
Figure 18 Broker Settings	22

#### **1. TECHNICAL SUPPORT**

For general contact, technical support, to report documentation errors and to order manuals, contact *BeanAir Technical Support Center* (BTSC) at:

#### tech-support@Beanair.com

For detailed information about where you can buy the Beanair equipment/software or for recommendations on accessories and components visit:

#### www.Beanair.com

To register for product news and announcements or for product questions contact Beanair's Technical Support Center (BTSC).

Our aim is to make this user manual as helpful as possible. Keep us informed of your comments and suggestions for improvements.

Beanair appreciates feedback from the users of our information.

## 2. VISUAL SYMBOLS DEFINITION

Symbols	Definition
	<u>Caution or Warning</u> – Alerts the user with important information about Beanair wireless sensor networks (WSN), if this information is not followed, the equipment /software may fail or malfunction.
	<u>Danger</u> – This information MUST be followed if not you may damage the equipment permanently or bodily injury may occur.
1	<u>Tip or Information</u> – Provides advice and suggestions that may be useful when installing Beanair Wireless Sensor Networks.

## 3. ACRONYMS AND ABBREVIATIONS

SSL	Secure Socket Layer
TLS	Transport Layer security
ССА	Clear Channel Assessment
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
GTS	Guaranteed Time-Slot
kSps	Kilo samples per second
LLC	Logical Link Control
LQI	Link quality indicator
LDCDA	Low duty cycle data acquisition
МАС	Media Access Control
PAN	Personal Area Network
PER	Packet error rate
RF	Radio Frequency
SD	Secure Digital
WSN	Wireless sensor Network

### 4. DOCUMENT ORGANIZATION



#### 5. MQTT CONFIGURATION

To Start configure MQTT, select your BeanDevice<sup>®</sup> Wilow<sup>®</sup> and go to the BeanDevice<sup>®</sup> Wilow<sup>®</sup> menu and scroll down to MQTT

 WebenScape

 File
 Server
 Tools
 Off. Data Analysis
 Advanced func.
 Help

 Mac\_int
 Mac\_int
 Mac\_int
 Enable measure log
 Disable measure log

 Mac\_int
 Ch\_X
 Disable measure log
 Clear graphs for all the sensors
 Display Wireless Network Information

 Sensor Configuration
 MQTT

Figure 1: BeanDevice® Wilow® menu

MQTT Module window will pop up as follow:

■ MQTT Module : MAC_ID : 0 x 5C313E06A9EC0000 -				
Broker	MQTT Status			
Port: 1883	MQTT Status: Stopped Stop Validate			
DNS Status: Enabled	MOTT Ack: NA			
IP Broker: 0.0.0.0	Indian Indian			
DNS: broker.hivemq.com	Topic for static measurement			
[ Import Validate	Publish Status: Disabled			
Authentication	ID Channel: 0 Ch_Z V			
Usemame:	Topic Name: Default			
Password:	Validate			
Validate				
SSL/TLS Config	l opic for dynamic measurement			
Security choice : Disabled Disabled T	MQTT Status: Enabled			
Security Protocol Version: SSLv3_0 SSLv3_0	Streaming Topic: 5C313E06A9EC0000/STREAMING Default			
Cichan Automatic	Validate			
	Subscription			
	Subscription status: Enabled			
Validate config	Tonio Name: 50313E0549E00100/0TAC Default			
Certificate :	Topic Name. Best best best of the Berault			
	Validate			
	Vere Alter			
	Interval : Gi			
Upload Status				
Start Start	Version: V3R1R1 V3R1R1 V			
Hoload Status Cancel and reset	Auto.gen.ID Client:			
Pito Transformd	ID Client: WILO5001581585302077803			
Progress 0%	Validate			
1 Togrood				

Figure 2: MQTT Module window

#### 5.1 BROKER

The broker is responsible for distributing messages to the related clients based on the topic of a message and there are two categories of brokers:

- Brokers hosted on the web
- ✓ Brokers running on the internal network.

Broker Port:	1883	1883
DNSStatus:	1	$\checkmark$
Brokerlp:	0.0.0.0	
DNS:		iot.eclipse.org
	Import	Validate

#### Figure 3: Broker frame

- Port: TCP/IP port to use with MQTT. 1883 and 8883 are the reserved ports for use with MQTT
- **DNSStatus:** check if you want to enter your broker DNS. DNSStaus is 1
- **Brokerlp**: enter your broker IP address after unchecking DNSStatus. DNSStatus is 0
- **DNS**: domain name server of your Broker

#### 5.2 KEEP ALIVE

The keep alive functionality assures that the connection is still open and both broker and client are connected to one another

KeepAlive		
Interval:	60	60
Version:	V3R1R1	V3R1R1 ~
Auto_gen_client_id_	1	$\checkmark$
Client ID:	WILO8425901549372612666	
		Validate

#### Figure 4: Keep alive frame

- **Interval**: The interval is the longest possible period of time, which broker and client can endure without sending a message.
- Version: MQTT protocol version
- Auto\_gen\_client\_ID: check for auto generate a Client ID

*Client ID*: Enter your client ID

#### 5.3 AUTHENTIFICATION

MQTT broker can be configured to require client authentication using a valid username and password before a connection is permitted.

Authentification	
User Name:	
Password:	
	Validate

Figure 5: Authentication frame

- User Name: specify your user name
- Password: enter your password
  - 5.4 SSL/TLS

**SSL** stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems. The two systems can be a server and a client. It does this by making sure that any data transferred between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.

**TLS** (Transport Layer Security) is a secured version of SSL.

Security choice : Disabled Enabled • Security Protocol Version: SSLv3_0 Automatic • Cipher : Automatic Automatic •	SSL/TLS Config			
Security Protocol Version: SSLv3_0 Automatic  Cipher: Automatic Automatic	Security choice :	Disabled	Enabled	•
Cipher : Automatic - Automatic	Security Protocol Version:	SSLv3_0	Automatic	•
Automatic -	Cipher :	Automatic		
		Automatic		-
Validate config		Validate config		

#### Figure 6 SSL/TLS

- *Security choice:* Enable or disable the security.
- *Security Protocol Version:* Choose the security protocol (Automatic choice is recommended).
- *Cipher:* Choose the cipher suit (Automatic choice is recommended).

#### TN\_RF\_021

#### 5.5 CERTIF

We can choose the server root file from the local machine.

Certif		
Certificate		📕 🕹 🕹
CA file Name :	NA	
CA file Valid from :	NA	
To	NA	
Upload Status		Start
File Status	NA	
Upload Status	NA	Cancel and reset
Byte Transferred		
Progress	0%	
	<u>Figure 7 Certif</u>	
Certificate: choose	the certificate from local machin	e.
CA file Names onto	with a name of the file	
<i>CA file Nume:</i> ente		
CA file Valid from:	choose the sender.	
<b>To:</b> choose the reconstruction of the recon	eiver (we can check the validity of	the file on the Beanscape side before send
Start: starting the p	process of the sending.	
Cancel and reset: o	ancelling the sending of the file a	nd reset the informations.
	11C	

- ✓ connected or stopped,
- $\checkmark$  connecting or disconnecting

And you can start your connection from here.

							 	_		
s: Conn	Connec	cted				Start	 $\sim$		Validat	е
k: Clien	Client A	ccepted							Restar	t
	Ŀ	Figure &	<u>8: MC</u>	<u>QTT St</u>	tatus j	frame				

MQTT Status: shows the current status of the MQTT module:

- Connecting: trying to establish a connection
- Connected: connection established
- Disconnecting: disconnecting the Client
- Stopped: the connection is stopped
- **Start/Stop:** select and **Validate** to start or stop your MQTT Client connection
- **Restart:** restart your connection

#### 5.7 TOPIC FOR STATIC MEASUREMENT

A topic is a string used by the broker to filter messages for each connected client. Using this Topic for static measurement you will receive LowDutyCycle & Alarm acquisition modes that are publishing to the MQTT broker,

<ul> <li>Topic for Static measure</li> </ul>	ment		
Publish_status:	Enabled	$\checkmark$	
Channel ID:	0	Ch_Z ~	
Topic Name:	F4B85E00A14B0000/SENSOR/0		Default
	F4B85E00A14B0000/SENSOR/0		Validate

Figure 9: Topic for static measurement frame

- Publish\_status: Check the check-button and validate to enable publishing
- **Channel ID:** channel identification
- **Topic Name:** Field to enter your topic's name

#### 5.8 TOPIC FOR DYNAMIC MEASUREMENT

Using this Topic for Dynamic measurement you will receive Streaming, S.E.T & Shock detection acquisition modes that are publishing to the MQTT broker,



Figure 10: Topic for dynamic measurement frame

- **Publish\_status:** check the check-button and **validate** to enable publishing
- **Streaming Topic:** Text field to enter your streaming topic's name

#### 5.9 SUBSCRIBE

subscribe_status:	Enabled		
Topic Name:	F4B85E00A14B0000/OTAC		Default
	F4B85E00A14B0000/OTA	с	Validate

- **Subscribe\_status:** check the check-button and **validate** to enable subscribing
- **Topic Name:** Field to enter your topic's name to subscribe to

#### 6. SSL CONFIGURATION

#### 6.1 INTRODUCTION ABOUT SSL

SSL stands for **S**ecure **S**ockets Layer and, in short, it is a standard technology for keeping an internet connection more secure and safeguarding any sensitive data that is being sent between two systems, preventing others from reading and modifying any information transferred, including any potential details. The two system can be server and client (for example, an application with personal identifiable information or with payroll information).

It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

TLS (Transport Layer Security) is an updated, more secure version of SSL. We still refer to our security certificates as SSL because it is more commonly used term.

#### 6.2 SSL ENCRYPTION FOR MQTT COMMUNICATION

#### Configuration on Beandevice<sup>®</sup> Wilow<sup>®</sup> Side

For **SSL** encryption over MQTT, the Beandevice<sup>®</sup> Wilow<sup>®</sup> is considered as the client here, and the broker act as a server. First of all we need to download <u>Root certificate CA</u> of the server into the Beandevice<sup>®</sup> Wilow<sup>®</sup>.



The Root certificate CA must be a binary file (\*.der format)

To convert any type of certificate to a binary file, we can use OpenSSL with the following command:



Figure 12 OpenSSL command

TN_RF_021			Wilow <sup>®</sup> w	rireless sensors series
	SSL/TLS Config Security choice :	Disabled	Enabled	•
	Security Protocol Version:	SSLv3_0	SSLv3_0	•
	Cipher :	Automatic		
				•
		Validate config		
		Figure 13 SSL/TLS configurati	ion	

On Beanscape<sup>®</sup> Wilow<sup>®</sup>, we need to enable the Security choice at first, then configure the secure socket, choose the Security protocol and the cypher in **"SSL/TLS config"** window.

It is highly recommended to choose the Automatic choice for both protocol and cypher then let the server and client choose the most appropriate configuration from the available parameters for both sides during the handshake process

After that in "certif" window we choose the server root file from the local machine and the most important thing is to verify the certificate validity (CA file valid from \ Ca file valid to) so we have put a filter (Beanscape side) to check the validity before we sent the file to avoid problems.

Finally, we click start to send the file.

#### Beanscape<sup>®</sup> Wilow<sup>®</sup> side

To configure the MQTT on the Beanscape side, we need to click on tools then choose MQTT configuration option:



Figure 14 MQTT configuration

For MQTT communication, Beanscape<sup>®</sup> Wilow<sup>®</sup> is also seen as a client from the broker side, like the BeanDevice<sup>®</sup> Wilow<sup>®</sup> the server root certificate is needed and then configure the secure socket options.

MQTT Configuration	n			
Use DNS				
DNS:	tailor.cloudmqt	t.com	tailor.cloudm	qtt.com
Broker IP	192.168.1.244		192.168.1.24	14
Port:	1884		1884	÷
Enable Authen	tication			
User Name			[[	
Password:				
Enable SSL				
SSL/TLS Version	TLSv1_2		TLSv1_2	•
	Validate		Clear all	
Certification tools				
Certificate	:\Program Files	(x86)\BeanScape	Wilow RA\cert	f\Sen 🕕 💭 🛅
Certif.State	stalled,Valid unt	il : 07/01/2025 1	4:19:29	
	Check	Install	Uninst	all

Figure 15 MQTT configuration window

On Beanscape<sup>®</sup> Wilow<sup>®</sup>, you can check if your certificate is already installed, if not, click on "install".

#### 6.3 SSL FOR OTAOP COMMUNICATION

#### Configuration on Beandevice<sup>®</sup> Wilow<sup>®</sup> Side

In this case, the device is the server here and Beanscape is the client. So for server, we need to have two main files: <u>Private key file and server certificate file.</u>

- ✓ For the private key file, it will be installed only one time into the device (no need to change it over the time, only for extreme security reason).
- ✓ For the server certificate file is also binary file (\*.der format).

These two files are supplied by BeanAir's team.

BeanDevices :: F45EABAF25FB0000 • • • • • • • • • • • • • • • • •	The state of the second second				~	and a second sec	1
Pile type : Certif AP   Upload Via WHP Image: Connected Selected BeanDevice ::   Connection Status Connection Protocol ::   Otwork Config Security choice ::   Security choice :: Disabled ·   Connection Protocol :: OtacOp ·   Verify Server:: No   Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\   Certif Certificate   C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\   Certif Certificate   C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\   ile Status	BeanDevices : F45EABAF	-25FB0000 -	💽 🛜 Switch to a	ccess point			
Upload Via Wi-R     Image: Connection Status     Disconnect     Selected BeanDevice :     Image: Connect     Security Choice :     Disconnect     Security Choice :     Disconnect     Security Choice :     Disconnect     Security Choice :     Disconnect     Security Protocol Version:   TLSv1_2   Security Protocol Version:   TLSv1_2   Security Protocol Version:   To:   Certificate   C:\Users\BeanairTeam1\Desktop\Omar Skander\Documenta\SSL\   Cafile Name   C=SE, O=AddTrust AB, OU=AddTrust   CA file Valid from :   30/05/2020 11:48:38   To:   30/05/2020 11:48:38     Upload Status   Ma   pload Status   Ma   pload Status   Ma   Statu     Ma     Progress     O%     Statu     Cancel and reset	File type : Certif AP	•	>				
onnection Status Deconnected     Connect Deconnection     Mathematic     Security Choice : Desabled     Security Protocol Version: TLS 12     Security Protocol Version: TLS 12     Verify Server: NO     Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Indicate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Indicate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\   Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\   Cafile Name C=SE, 0=AddTrust AB, 0U=AddTrust   CA file Valid from: 30/05/2000 11:48:38   To: 30/05/2020 11:48:38     Upload Status     Mathematic     Verify Fransferred   Cancel and reset	) Upload Via Wi-Fi		Upload Via TCP/MQ	Π			
Connect Disconnect     New Config   Security choice :   Disabled   Connection Protocol :   OtacOp   Verify Server:   NO   Cipher :   Automatic     Certificate   C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\   Cafile Name   C=SE, O=AddTrust AB, OU=AddTru   CA file Valid from :   30/05/2000 11:48:38   To :   30/05/2020 11:48:38   Upload Status   NA   upload Status   NA   Cransferred   Progress   O%	onnection Status	nected	Selected BeanDevice	:			
New Config  Security choice : Disabled   Connection Protocol : OtacOp  Validate Security Protocol Version: TLSv1_2  Security Protocol : TLS  Verify Server: NO  Cipher : Automatic  Certif Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\ CA file Name C=SE, O=AddTrust AB, OU=AddTru CA file Valid from : 30/05/2000 11:48:38  To : 30/05/2020 11:48:38  Upload Status NA Ipload Status NA Statu Of Cancel and reset	Co	nnect Disconnec	t NA				
Security choice : Disabled   Connection Protocol : OtacOp  Validate  Security Protocol Version : TLSv1_2  Security Protocol : TLS  Verify Server: NO  Cipher : Automatic  Certif  Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\ CA file Name C=SE, O=AddTrust AB, OU=AddTru CA file Valid from : 30/05/2000 11:48:38  To : 30/05/2020 11:48:38  Jpload Status  ile Status  NA  verify Server: NA  Cancel and reset	New Config	100					
Security Protocol Version: TLSv1_2   Verify Server: NO  Cipher: Automatic  Certif  Certificate  C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\ CA file Name C=SE, O=AddTrust AB, OU=AddTru CA file Valid from: 30/05/2000 11:48:38  To: 30/05/2020 11:48:38  Joload Status  Joload Status  VA  Verify Start  Cancel and reset	Security choice : Dis	abled 🔻	Connection Protocol : Ota	acOp 🝷	Validate		
Verry Server: NO     Cipher: Automatic     Certif Certificate     C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\     CA file Name C=SE, 0=AddTrust AB, OU=AddTru   CA file Valid from: 30/05/2000 11:48:38   To:   30/05/2020 11:48:38   Upload Status   VA   Upload Status   VA   Upload Status   VA   Of the transferred   Of transferred	Security Protocol Version: TL	Sv1_2 •	Security Protocol : TL	S 💽			
Certificate C:\Users\BeanairTeam1\Desktop\Omar Skander\Documents\SSL\ CA file Name C=SE, O=AddTrust AB, OU=AddTr. CA file Valid from : 30/05/2000 11:48:38 To : 30/05/2020 11:48:38 Upload Status File Status NA Joload Status NA Upload Status		· · · ·	Cipher : Automatic		· · ·		
CA file Name C=SE, O=AddTrust AB, OU=AddTru CA file Valid from : 30/05/2000 11:48:38 To : 30/05/2020 11:48:38 Upload Status File Status NA Upload Status NA Syte Transferred 0% Start Cancel and reset	Certif Certificate C:V	Users\BeanairTeam1\De	sktop\Omar Skander\Document	s\SSL\ 📮 🛃			
CA file Valid from : 30/05/2000 11:48:38 To : 30/05/2020 11:48:38 Upload Status File Status NA Upload Status NA Optor Transferred Progress 0% Start Cancel and reset	CA file Name C=S	SE, O=AddTrust AB, OU=	AddTru				
Upload Status File Status Upload Status Upload Status NA Upload Status NA	CA file Valid from : 30/	05/2000 11:48:38	To : 30/05/2020 1	1:48:38			
File Status     NA       Upload Status     NA       Byte Transferred     Image: Cancel and reset	Upload Status						
NA       Upload Status     NA       Byte Transferred     Image: Cancel and reset							
Upload Status NA Byte Transferred 0% Progress 0% Start Cancel and reset	File Status						
Byte Transferred  Progress Cancel and reset	Upload Status						
Progress 0% Start Cancel and reset	Byte Transferred						
Start Cancel and reset	Progress		0%				
		0-4					

Figure 16 firmware uploader

On Beanscape<sup>®</sup>, we select the access point (AP) certificate as an option for file to be uploaded to the device, after that we choose the file from the local machine and click start to send file.

Please note it is preferred to not change any configurations related to the secure socket options.

#### Beanscape<sup>®</sup> Wilow<sup>®</sup> side

The Beanscape<sup>®</sup> Wilow<sup>®</sup> is a client in this case, so it needs only the Root certificate file of the device, this file is saved inside Beanscape folders.

#### 6.4 SSL FOR BEANSCAPE® WILOW®

#### <u>Configuration on Beandevice® Wilow® Side</u>

This is a secure communication for our standard communication between Beanscape and all the devices, the principals are the same here, Beanscape is the server and the devices are clients.

As the device is a client it needs only the Root Certificate of the server, also it must be a binary file before we downloaded into the devices.

#### Beanscape<sup>®</sup> Wilow<sup>®</sup> side

Like mentioned before, the Beanscape<sup>®</sup> Wilow<sup>®</sup> is operating as a server here, so it needs two main things:

- ✓ the server certificate which will be installed inside Beanscape folders.
- ✓ the private key will be also installed in Beanscape folders.

#### 6.5 EXAMPLE OF MQTT BROKER ON TELTONIKA ROUTER (RUT240/RUT950)

For the MQTT communication between Beanscape<sup>®</sup> Wilow<sup>®</sup> and the BeanDevice<sup>®</sup> Wilow<sup>®</sup>, we can use the hosted broker on Teltonika Router RUT240/RUT950.

Like any kind of MQTT Broker, the router is acting as a server and both Beanscape<sup>®</sup> Wilow<sup>®</sup> and BeanDevice<sup>®</sup> Wilow<sup>®</sup> are acting as a client.

On the Teltonika broker configuration, we need to follow those steps:

- Enable the broker and specify the port ID ;

	Publisher		
QTT B	roker		
		Enable	
		Local Port	1884
		Enable Remote Access	

# Enable TLS/SSL option and update the 3 files:

Security	Bridge	Miscellaneous	
		Use TLS/SSL	
		CA File	Uploaded File (1.30 KB)
		CERT File	Uploaded File (1.21 KB)
		Key File	Uploaded File (1.64 KB)
		TLS version	Support all

#### Figure 18 Broker Settings

- ✓ **CA File**: the root CA file of the client, the server may request the client certificate to verify it.
- ✓ **CERT file**: the server certificate
- ✓ **Key File:** the server private key.