

1. Introduction

All of Infinite's devices that support the MQTT protocol, are capable to connect to any local or remote MQTT Broker. Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing deploying, and managing applications and services through Microsoft-managed centers.

This document is a brief how-to guide for all device communications between Infinite's devices and Microsoft Azure.

2. Generating Self-Signed Device Certificate and Key

Azure requires TLS communications so we will have to create our own self-signed certificate and key for our device. We do that with the commercial-grade TLS toolkit `openssl`. The easiest way to do that is to simply install [git](#) on your computer and locate the `openssl.exe` file in this directory: `C:\Program Files\Git\usr\bin\openssl.exe`.

Open a Command Prompt or PowerShell window in the above directory and type the following commands to create the device certificate and key:

```
req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout device.key -out device.crt
```

- creates device certificate and private key

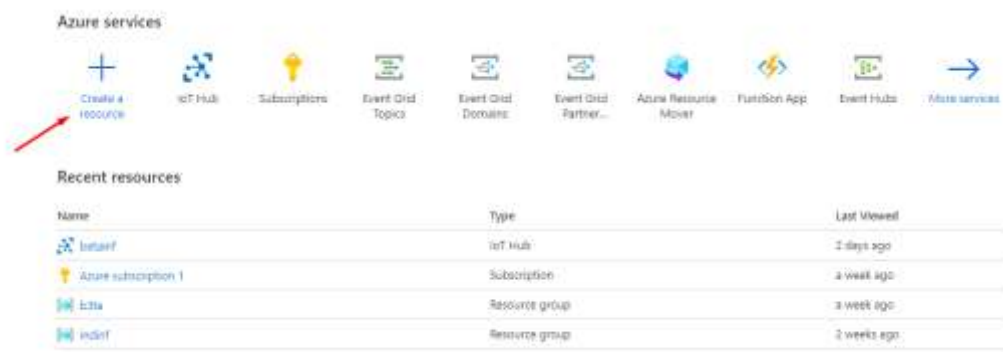
In the same window, create a .PEM file from your certificate:

```
x509 -in device.crt -out device.pem -outform PEM
```

(These commands are for testing purposes and should be adjusted for different requirements.)

3. Creating an IoT Hub

After creating a Microsoft Account, the first step of this procedure is to create an IoT Hub. On the homepage of Microsoft Azure, click Create a resource and then search for IoT Hub.



Create an IoT Hub by filling out the project details and creating a new Resource group. You must choose East US as your region for the time being as Microsoft is working on enabling TLS1.2 on all regions.

MQTT - Connecting to Microsoft Azure

Home > Create a resource > IoT Hub >

IoT hub

Microsoft

Basics Networking Management Tags Review + create

Create an IoT hub to help you connect, monitor, and manage billions of your IoT assets. [Learn more](#)

Project details
Choose the subscription you'll use to manage deployments and costs. Use resource groups like folders to help you organize and manage resources.

Subscription * ⓘ Azure subscription 1 ▼

Resource group * ⓘ indmf ▼
[Create new](#)

Instance details


IoT hub name * ⓘ MyVeryFirstHub ✓

Region * ⓘ East US ▼



[Review + create](#) < Previous Next: Networking >


Make sure that you configure the minimum TLS version as well.



MQTT - Connecting to Microsoft Azure

IoT hub 


Scale tier and units

Pricing and scale tier  F1: Free tier 









 Free IoT hubs are limited to one per subscription
[Learn how to choose the right IoT hub tier for your solution](#)

Number of F1 IoT hub units   1

Determines how your IoT hub can scale. You can change this later if your needs increase.



Defender for IoT  Off

Turn on Defender for IoT and add an extra layer of threat protection to IoT Hub, IoT Edge, and your devices. [Learn more](#)


Pricing and scale tier 	F1	Device-to-cloud messages 	Enabled
Messages per day 	8,000	Message routing 	Enabled
Cost per month:	0.00 EUR	Cloud-to-device commands 	Enabled
Defender for IoT 	Disabled	IoT Edge 	Enabled
		Device management 	Enabled


Advanced settings

Scale

Device-to-cloud partitions   2

Transport Layer Security (TLS)

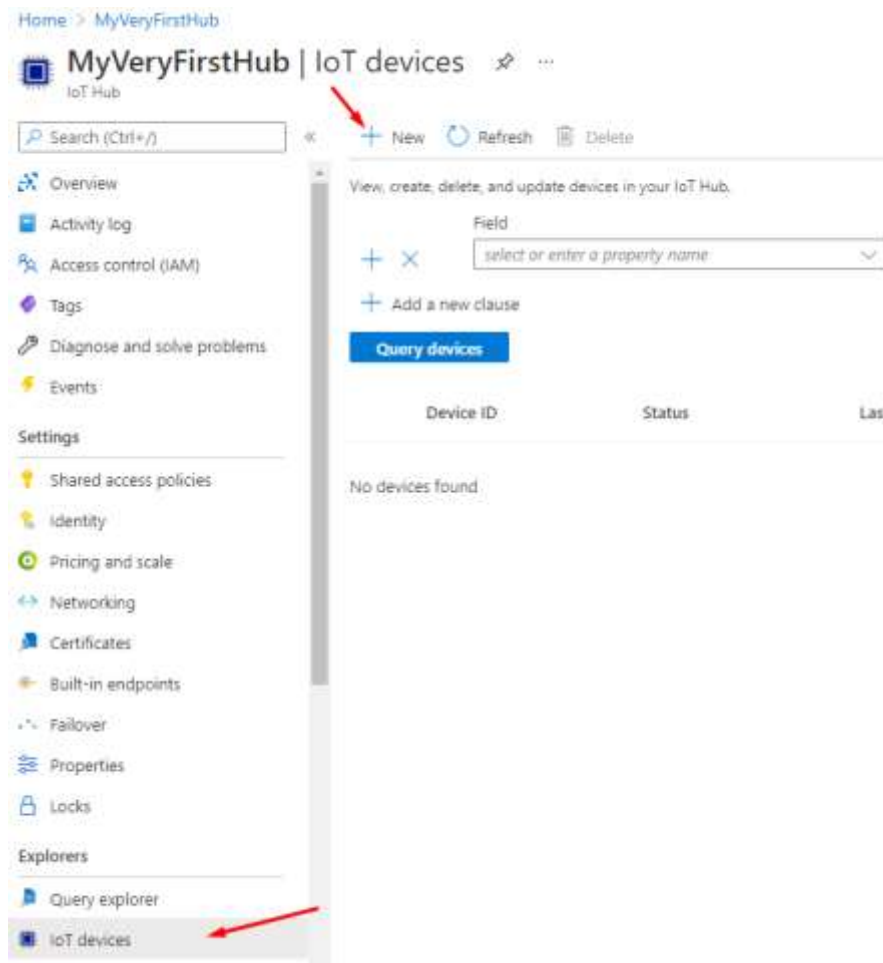
Minimum TLS Version  ☐ 1.0 ☒ 1.2



[Review + create](#) [Previous: Networking](#) [Next: Tags >](#)

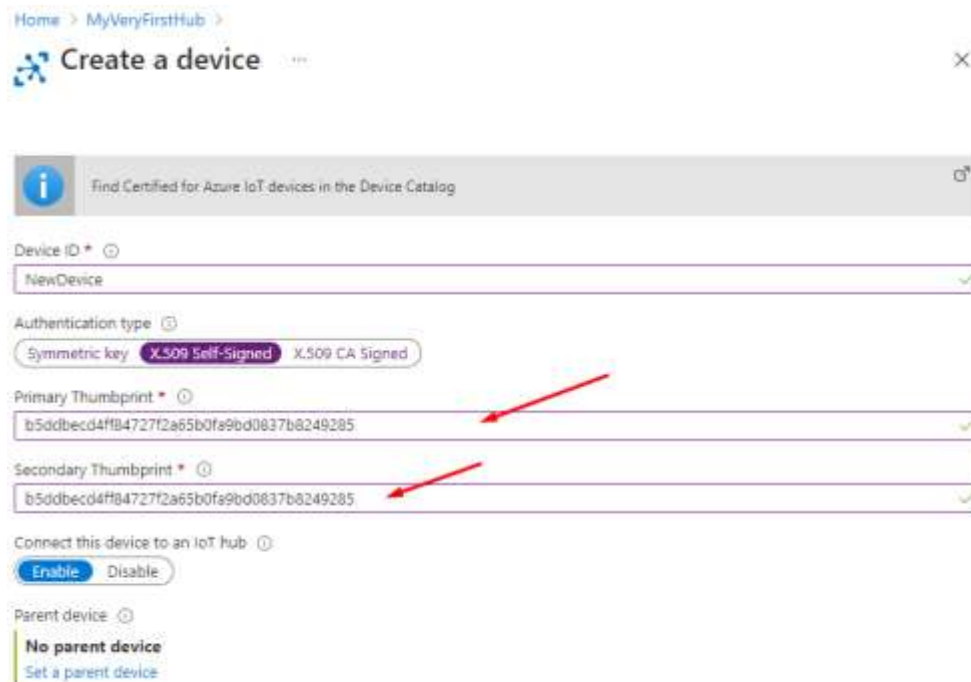
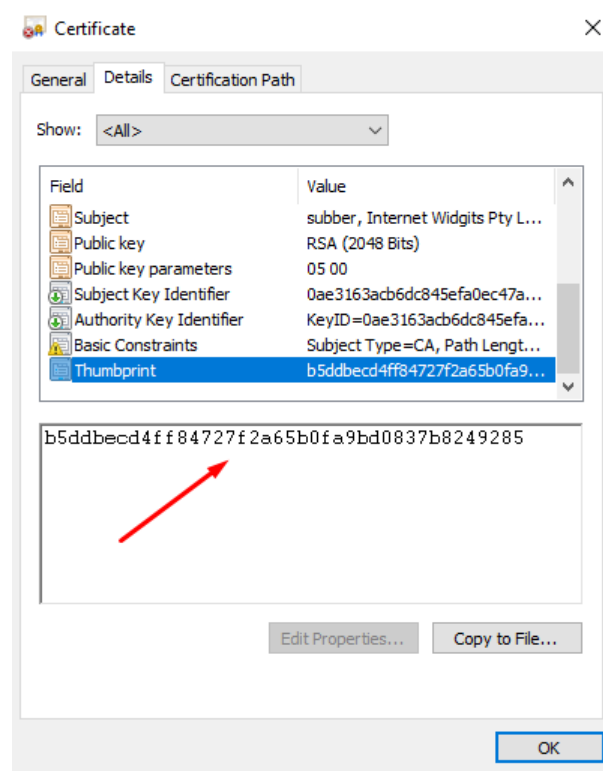
3.1 Creating a device

While you are on your IoT Hub page, enter the IoT devices tab and click New to create an IoT device.



On the next page name your device, choose X.509 Self-Signed as the authentication type and enter your certificates Primary Thumbprint. You can find this thumbprint by opening the device.crt file we created earlier.

MQTT - Connecting to Microsoft Azure



4. Add Certificate

While you are on your IoT Hub page, enter the Certificates tab and click Add.

Upload the .PEM file that you previously created.

The image shows two screenshots from the Azure IoT Hub interface. The top screenshot displays the 'thermos | Certificates' page with a sidebar menu. A red arrow points to the 'Certificates' option in the menu. The bottom screenshot shows the 'Add certificate' dialog box. A red arrow points to the 'Add' button at the bottom left of the dialog, and another red arrow points to the 'Get certificate status to verified on upload' checkbox, which is checked.

thermos | Certificates
IoT Hub

Search (Ctrl+F)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Events
- Settings
 - Shared access policies
 - Identity
 - Pricing and scale
 - Networking
 - Certificates**
 - Built-in endpoints
 - Firmware
 - Properties
 - Locks
- Explorers
 - Query explorer
 - IoT devices

Upload and manage certificates for device authentication here. [Learn more](#)

When you upload a new certificate, we can automatically verify it for you (note that the status of existing certificates won't change). [Learn more](#)

+ Add Refresh

Name	Created	Expires	Subject	Thumbnail
------	---------	---------	---------	-----------

Add certificate

Certificate name *

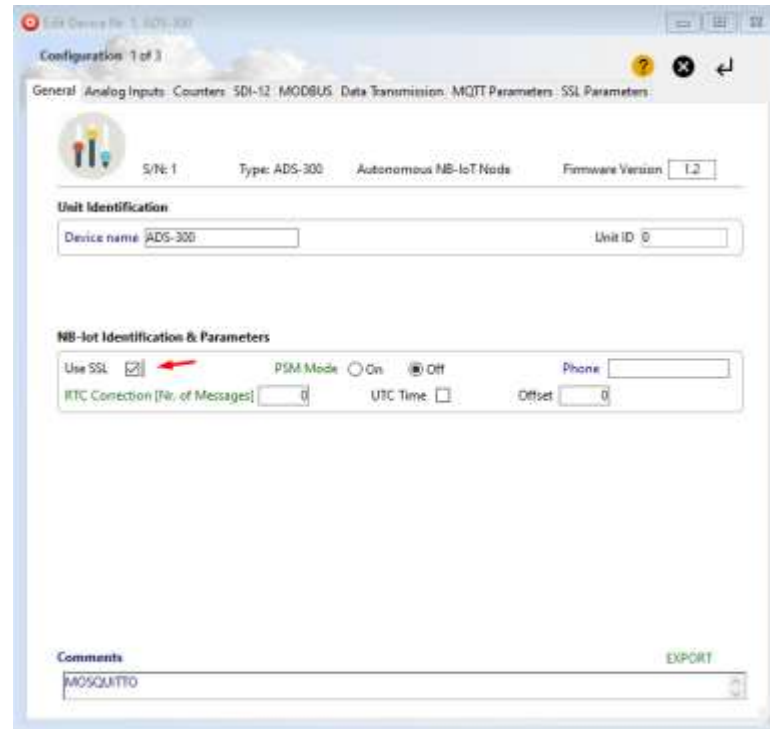
Certificate path or url file

☒ Get certificate status to verified on upload

We'll verify this certificate automatically, with no manual verification steps required. [Learn more](#)

5. Device Configuration with WA Manager

In the Edit Device window in WA Manager, tick the Use SSL box.



Next, we configure the MQTT parameters.

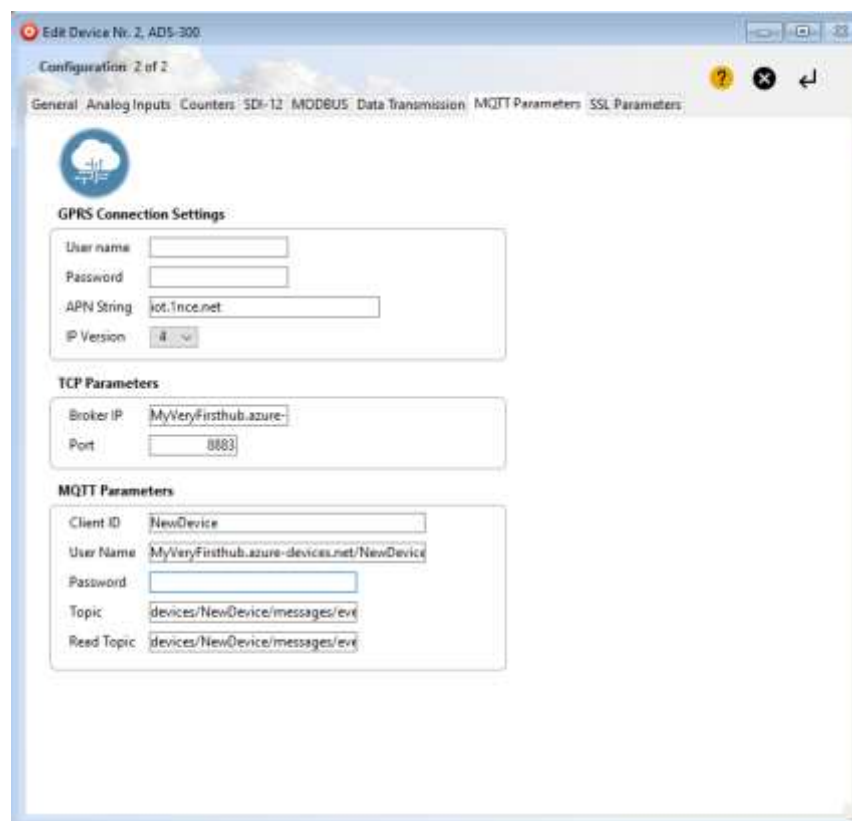
Although Azure supports MQTT connectivity, it is not a pure MQTT Broker and so it has some limitations regarding its MQTT parameters.

For the Broker IP, the IoT Hub endpoint must be used that can be found in the IoT Hub page.



MQTT - Connecting to Microsoft Azure

For the Client ID, the Device ID must be used that we used to create our device.



The screenshot shows the 'Edit Device' configuration window for 'ADS-300'. The 'MQTT Parameters' tab is selected. The configuration is as follows:

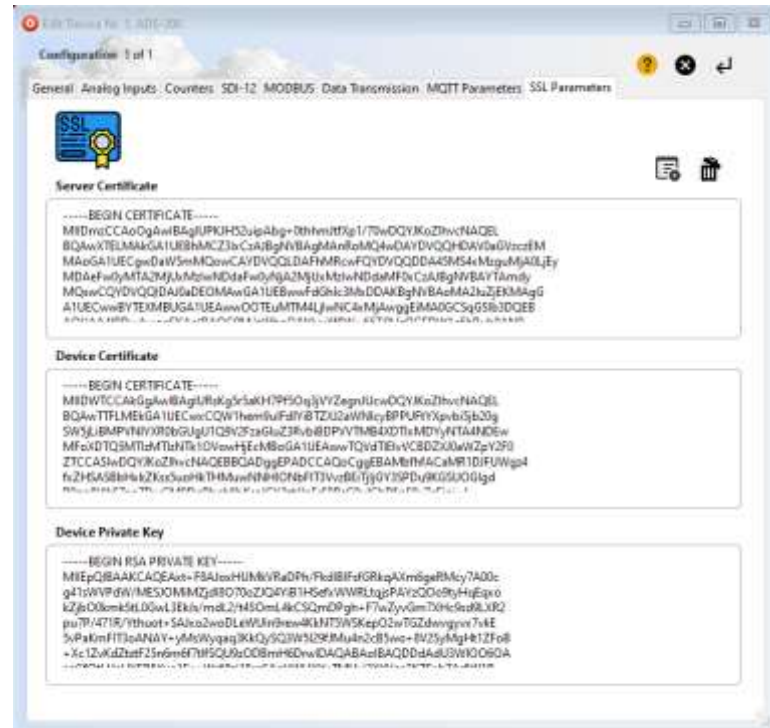
Section	Field	Value
GPRS Connection Settings	User name	
	Password	
	APN String	iot.fince.net
	IP Version	4
TCP Parameters	Broker IP	MyVeryFirsthub.azure-
	Port	8883
MQTT Parameters	Client ID	NewDevice
	User Name	MyVeryFirsthub.azure-devices.net/NewDevice
	Password	
	Topic	devices/NewDevice/messages/ev
	Read Topic	devices/NewDevice/messages/ev

The username must be of this format based on the name of our DeviceID and IoT Hub name: `{IoThubname}/{deviceid}?api-version=2018-06-30`

The topic must be of this format: `devices/{deviceid}/messages/events/`

Lastly, in the SSL Parameters tab, we copy and paste the three files needed for the TLS communication: Server Certificate (CA), Device Certificate and Device Private Key.

MQTT - Connecting to Microsoft Azure



The Server Certificate is [this](#) Digicert CA, the Device Certificate is the device.crt file and the Device Private Key is the device.key file. These files should be first opened with Notepad++ and their contents should be copy and pasted in the above tab. All files must be PEM formatted.

4. Load Certificates via Terminal

Alternatively, the certificates can also be loaded via a terminal program of your choice. This example uses Tera Term.

The serial port settings are shown in the image below.

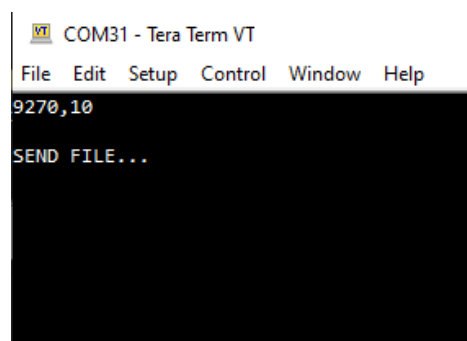
Speed:	115200
Data:	8 bit
Parity:	none
Stop bits:	1 bit
Flow control:	none

The commands for sending each of the certificates are shown in the table below.

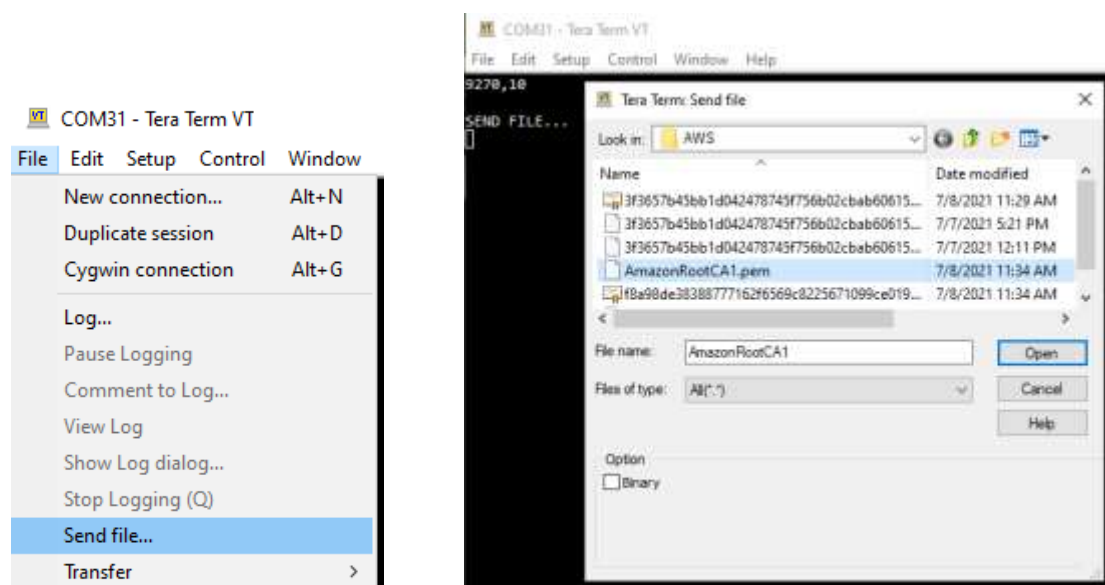
MQTT - Connecting to Microsoft Azure

9270	Send SSL Certificates	cmd,n	n: 10: Root Certificate, 20: Device Certificate, 30: Device Private Key
------	-----------------------	-------	---

So, for sending the Root Certificate we should enter the command **9270,10** in the terminal.



Then, send the appropriate file.



And enter the special character *. This is achieved by pressing Ctrl+8.

```
COM31 - Tera Term VT
File Edit Setup Control Window Help
9270,10

SEND FILE...
-----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPm1jZbyjANBgkqhkiG9w0BAQsF
ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBBWF6
b24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
MAkGA1UEBhMCVVMxMzANBgNVBAoTBkFtYXpvcjEzMjcGA1UEAxMQQW1hem9uIFJv
b3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ca9HgFB0fw7Y14h29Jlo91ghYP10hAEvrAItht0gQ3p0sqTQNroBvo3b5MgHFzZM
906II8c+6zf1tRn4SWiw3te5djgdYZ6k/oI2peVKVuRF4fn9tBb6dNqcmzU5L/qw
IFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRwa6
VOUjw5H5SNz/0egwLX0tdHA114gk957EWw67c4cX8jJGKLhD+rcdqsq08p8kD11L
93FcXmn/6pUCyziKrLA4b9v7LWIBxcceVOF34GfID5yHI9Y/QCB/IIDEgEw+OyQm
jgSubJrIqg0CAwEAANCMCAwDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8EBAMC
AYYwHQYDVIR00BBYEFIQYzIU07LwM1JQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBChUA
A4IBAQC8Y8jdaQZChGsV2USggNiM0ruYou6r4lK5IpDB/G/wkjUu0yKGX9rbxenDI
U5PMCCjJmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxh1bI1BjJt/msv0tadQ1wUs
N+gDS63pYaACbvXy8Mwy7Vu33PqUXHeeE6V/Uq2V8viT096LXFvKW1JbYK8U90vv
o/ufQJVTMT8QtPHRh8jrdkPSHca2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
5MsI+yMRQ+hDKXJioa1dXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
rQXRfboQnoZsG4q5WTP468SQvvG5
-----END CERTIFICATE-----
*COMMAND PROCESSED OK
█
```

The device will answer with the message **COMMAND PROCESSED OK** if the configuration was successful.

Do the same for the other two certificates with their respective commands.

Your device can now connect Azure and send your encrypted data safely.

Disclaimer:

Azure is a registered trademark of Microsoft Corporation, USA. All products and software mentioned in this document for educational and demonstration purposes.

Revision: 1.2

© 2021, Infinite Informatics Ltd

Infinite Informatics, Ltd

1, Valaoritou Street
GR-54626 Thessaloniki, Greece
Phone: +30-2310-553545
E: info@indinf.gr
W: www.infinite.com.gr