RAK475 Use Guidance
How to Upload the SSL Certificate

Shenzhen Rakwireless Technology Co., Ltd.

www.rakwireless.com

info@rakwireless.com

1. Uploading the SSL Certificate via Web

1.1 Overview

This document presents two ways of uploading the SSL certificate required by the module – uploading via web and via AT assistant commands.

1.2 Operating instructions

Tips:

1. This demo is done on the RAK475 development board.
2. The module in this demo is under factory settings.
3. When sending command to control the module via MCU, enter "\r\n" to complete the command;
4. When sending command to control the module via the serial port tool, press Enter to complete the command;
5. For ease of viewing, the information returned by the send command is presented in ASCII value. Special characters or Chinese characters in the returned information might result in the information being partially displayed or unreadable. In these cases, please view the returned information in hexadecimal form.

Please keep in mind the abovementioned points, for they will not be mentioned later.

1.3 Creating an AP

1. The module is in AP Mode under the default factory settings
2. Refer to **RAK475 User Guide – Creating an AP Network**, create an AP
3. If the module needs to use the certificate in STA Mode, you can first upload the SSL certificate in AP Mode and then set the module to STA Mode

1.4 Steps

1.When you power on the module in Factory Mode, it will set up an open AP network named **RAK475_AP_XXXXXX** with a default IP address of **192.168.7.1**, and its **DHCP Server** function is enabled by default (factory parameters can be modified). After the **Status indicator** lights up, turn on the computer's wireless network, and **RAK475_AP_XXXXXX** can be found in the list of wireless networks, as shown in Figure 1-1:

Figure 1-1: Factory AP Scanning

2. Double click to join this network (the **Link indicator** will light up). Once its IP address is successfully assigned, open the browser and enter the module's gateway address **192.168.7.1**. In the pop-up authentication interface, enter the default **username: admin** and **password: admin**. As shown in Figure 1-2:
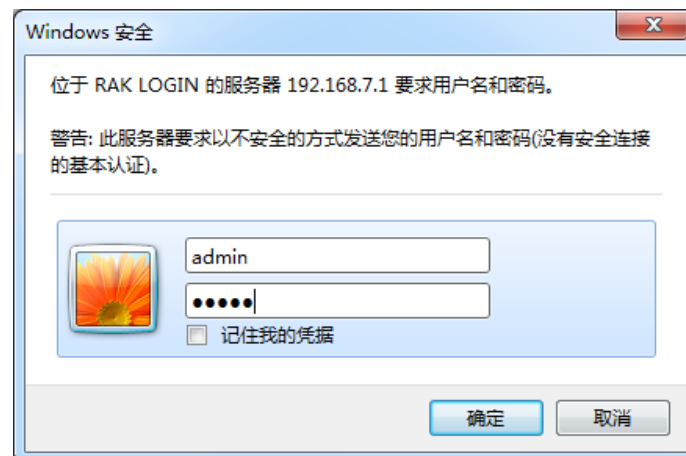

Figure 1-2: WEB Authentication

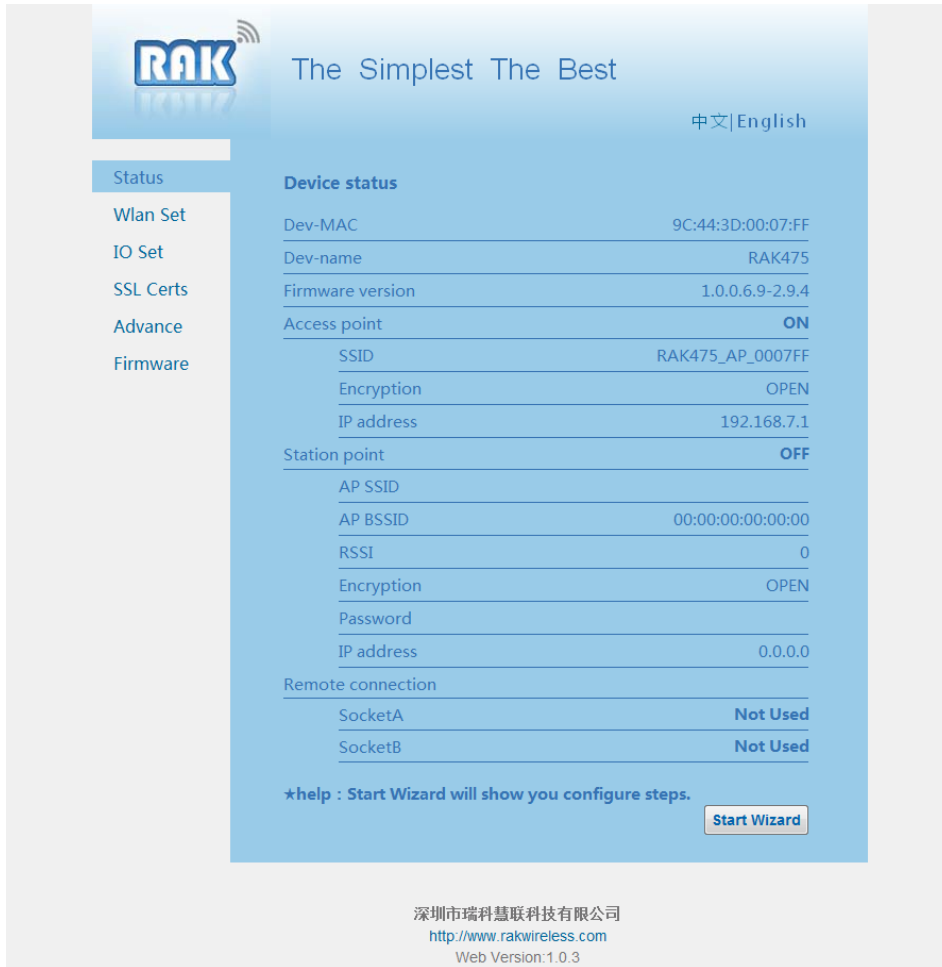3.Click **OK** to enter the **WEB Server** configuration page.

Figure 1-3 WEB Server Configuration Page

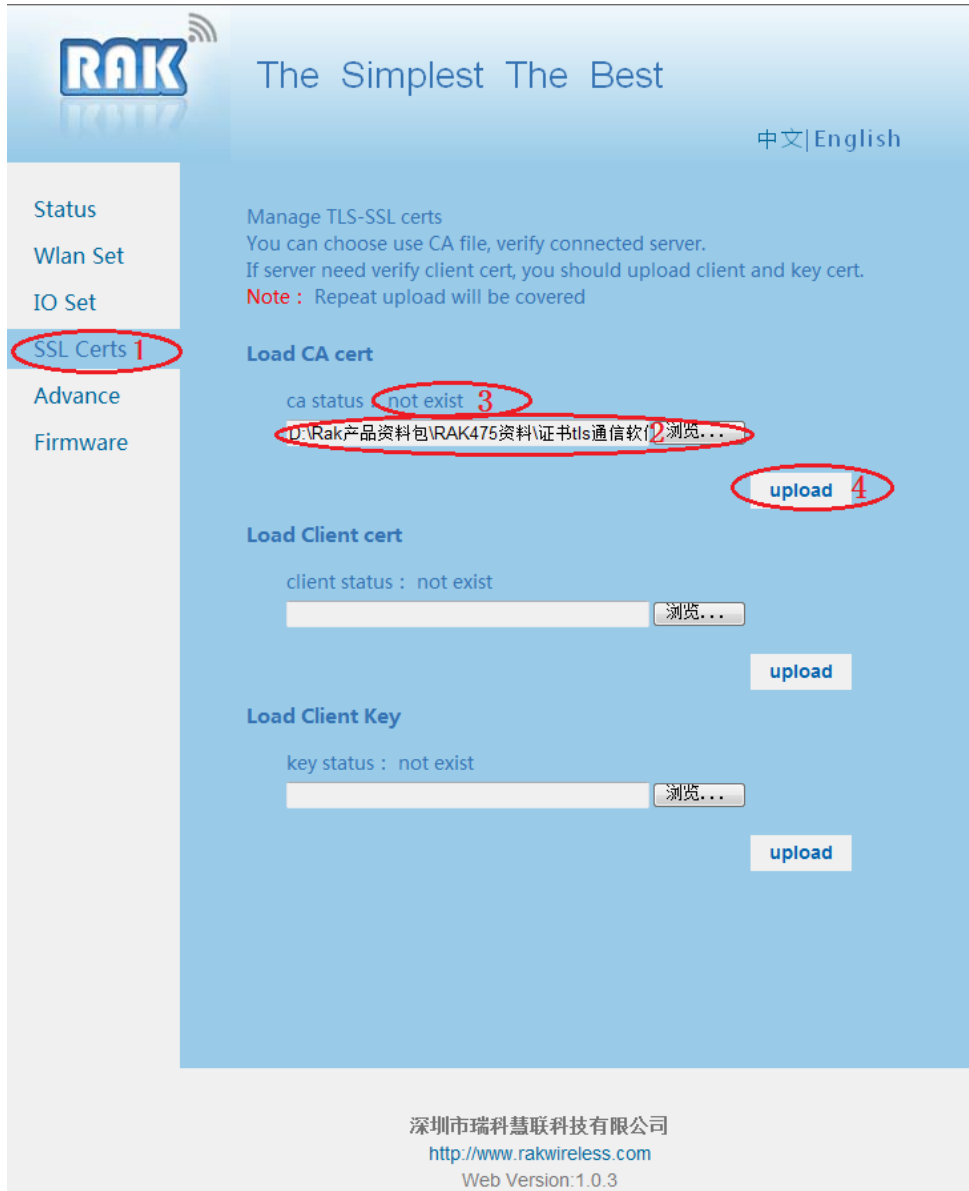4. Click the **SSL Certs** tab to enter the **Certificate Upload** page.

Figure 1-4 Certificate Upload Page

1) Click the **SSL Certs** tab to enter the certificate upload page;

2) Here we will upload **CA cert** as an example. Click the 浏览... button to set the path of the CA cert certificate;

3) When the certificate has not been uploaded, the status is displayed as "**no exist**";

4) Click **"upload"** to upload the certificate.

5. When the certificate upload is completed, the page will jump and display **"File upload successfully"** to indicate that the CA cert has been uploaded successfully. Click the **SSL Certs** tab again and repeat the above steps to upload the remaining certificates
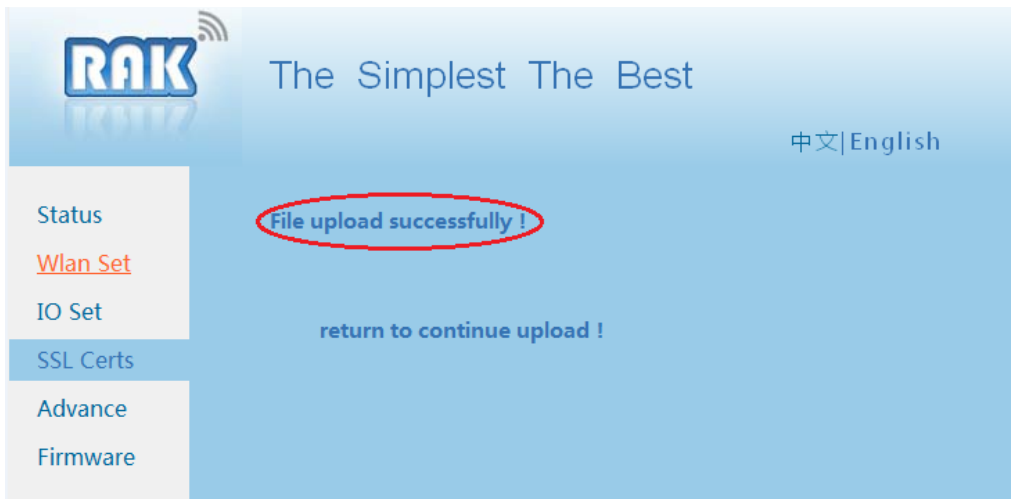
Figure 1-5 Certificate Upload Successful

2. Setting up the SSL Certificate via AT Assistant Command

2.1 Overview

In the exemplary process in this section, we set up the SSL certificate for the module using AT assistant command.

2.2 Operating instructions

Tips:
6. This demo is done on the RAK475 development board.
7. The module in this demo is under factory settings.
8. When sending command to control the module via MCU, enter "\r\n" to complete the command;
9. When sending command to control the module via the serial port tool, press Enter to complete the command;
10. For ease of viewing, the information returned by the send command is presented in ASCII value. Special characters or Chinese characters in the returned information might result in the information being partially displayed or unreadable. In these cases, please view the returned information in hexadecimal form.

Please keep in mind the abovementioned points, for they will not be mentioned later.

2.3 Steps

1) Enabling Assistant Command

Enabling the assistant command interface in Transparent Transmission Mode is done in a similar way to "handshake". As shown in Figure 2-1.

1. The host computer (master MCU) requests to enter Command Mode by sending "+++".

2. Set the timer for 200ms and wait for the module to return "U" (0x55) within this specified time. If the module did not return a "U" when the timer expires, send "+++" again until a "U" (0x55) is returned. Now the module is ready to enter Command Mode, and it is waiting for the final confirmation (wait for 3s).

3. After receiving the "U" (0x55), the host computer (master MCU) has to send a "U" (0x55) to the module as the last confirmation message within 3 seconds. If the module successfully received the confirmation message, it would return an "OK" and enter Command Mode. Otherwise, the module would exit the READY status and would be waiting for the next REQUEST command. In this case, repeat steps 1-3.
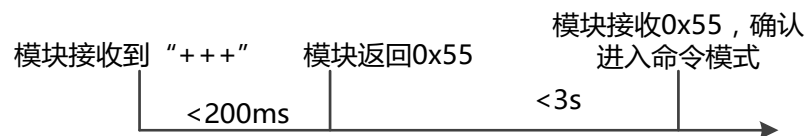
模块接收0x55，确认
模块接收到 "+++"   模块返回0x55   进入命令模式

<200ms   <3s

Figure 2-1 Enter Command Sequence

2) Setting up the SSL Certificate for the Module

Send: at+set_cert=<cert_type>,<file_len>,<data_stream>\r\n

Return: OK

（1）<cert_type>：Certificate Type　"0" SSL Client Private Key

"1" SSL Client Certificate

"2" SSL CA Certificate

（2）<file_len>：Certificate Byte Length, less than 4 * 1024 is required

（3）<data_stream>: Specific Certificate Strings

Refer to "**RAK475 User Manual**" for the details of the command parameters.

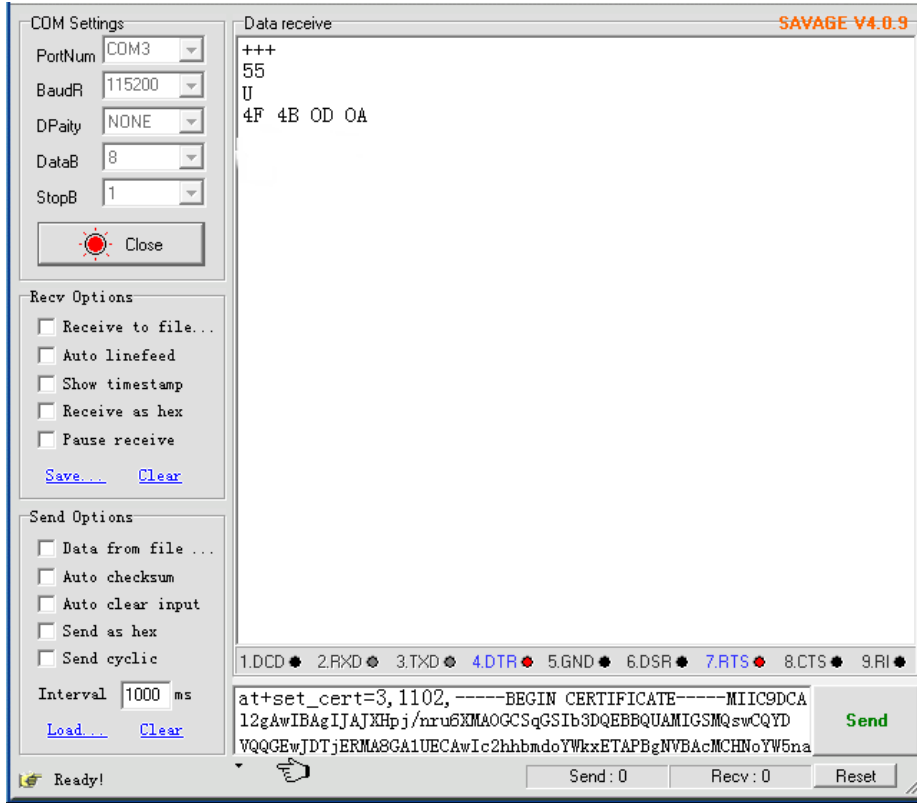3) As an example, Figure 2-2 shows how to set up the SSL CA Certificate

Figure 2-2

3

Version

Version	Author	Date	Content modification
V1.0	RAK	2016/12/06	Create a document