AT Command Options when Using TCP-SSL/TLS

1. Selecting Active Certificate Set

Use the 'PF' command to select which certificate is active for TCP_TLS.

There are 3 certificate sets that can be selected. This selection sets which set is active for a TCP-TLS connection and for programming via the 'PG' command.

2. Options for Programming a Certificate Set (RootCA, Certificates and Keys)

a. Use the eS-WiFi Demo tool to add the RootCA, Certificate, and Key to the bin file and then flash the module with the new bin file.

b. Use the eS-WiFi Demo tool and the 'PG' command to write the RootCA, Certificate, and Key into the flash on the module.

c. Use the Host microprocessor and the ''PG' command to write the RootCA, Certificate, and Key into the flash on the module.

Note: f you want to verify that the certificate set with 'PG' command is programmed correctly,

write the same RootCA, Certificate, or Key to the same certificate set and the result will be a match or an error.

* Please note that the certificate sets are OTP (One Time Programmable). Once all sets have been programmed the only way to clear them is to flash a complete firmware (not just an update firmware).

3. Verification Options

a. The 'P9' command sets the verification options for a TCP-TLS connection.

0 - No verification, uses the Certificate and Key supplied by the server.

1 - Optional Simple Context), uses the Certificate and Key supplied by the server, if a RootCA is program for the Certificate set it will be used to verify the server certificate.

2 - Required (Advance Context), uses the RootCA, Certificate, and Key in the certificate set to verify the server certificate and for the communication.

TLS CA/Certificate/Key Example

```
PF=0                                        //Certificate set 0
PG=0,0,<length>,<Root CA data bytes>        //RootCA
PG=0,1,<length>,<Cerificate data bytes>     //Certificate
PG=0,2,<length>,<Key data bytes>            //Key
```

TLS Client Examples:

1. Client to TLS Server, with server sending certificate and key to client (ex. Web Email)

```
P1=3                                        //TCP SSL/TLS
D0=<server domain or IP address>            //Get IP address of server
P4=<server port>                            //Server port*
P9=0                                        //No Verification
P6=1                                        //Start
```

2. Client to TLS Server, with RootCA verification

```
P1=3                                        //TCP SSL/TLS
D0=<server domain or IP address>            //Get IP address of server
P4=<server port>                            //Server port*
P9=1                                        //RootCA (if programmed)
P6=1                                        //Start
```

3. Client to TLS Server, with certificate verification

```
P1=3                                        //TCP SSL/TLS
D0=<server domain or IP address>            //Get IP address of server
P4=<server port>                            //Server port*
P9=2                                        //Verification
P6=1                                        //Start
```

*Note: The port numbers in the range from 0 to 1023 are the well-known ports or system ports. They are used by system processes that provide widely used types of network services. **Port 443** is the official Hypertext Transfer Protocol over TLS/SSL (HTTPS).