SIM7500_SIM7600_SIM7800 Series_SSL_Application Note

LTE Module

SIMCom Wireless Solutions Limited
Building B, SIM Technology Building, No.633, Jinzhong Road
Changning District, Shanghai P.R. China
Tel: 86-21-31575100
support@simcom.com
www.simcom.com

Document Title:	SIM7500_SIM7600_SIM7800 Series_SSL_Application Note
Version:	2.00
Date:	2020.8.6
Status:	Released

GENERAL NOTES

SIMCOM OFFERS THIS INFORMATION AS A SERVICE TO ITS CUSTOMERS, TO SUPPORT APPLICATION AND ENGINEERING EFFORTS THAT USE THE PRODUCTS DESIGNED BY SIMCOM. THE INFORMATION PROVIDED IS BASED UPON REQUIREMENTS SPECIFICALLY PROVIDED TO SIMCOM BY THE CUSTOMERS. SIMCOM HAS NOT UNDERTAKEN ANY INDEPENDENT SEARCH FOR ADDITIONAL RELEVANT INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE IN THE CUSTOMER'S POSSESSION. FURTHERMORE, SYSTEM VALIDATION OF THIS PRODUCT DESIGNED BY SIMCOM WITHIN A LARGER ELECTRONIC SYSTEM REMAINS THE RESPONSIBILITY OF THE CUSTOMER OR THE CUSTOMER'S SYSTEM INTEGRATOR. ALL SPECIFICATIONS SUPPLIED HEREIN ARE SUBJECT TO CHANGE.

COPYRIGHT

SIMCom Wireless Solutions Limited
Building B, SIM Technology Building, No.633 Jinzhong Road, Changning District, Shanghai P.R. China
Tel: +86 21 31575100
Email: simcom@simcom.com

For more information, please visit:
https://www.simcom.com/download/list-863-en.html

For technical support, or to report documentation errors, please visit:
https://www.simcom.com/ask/ or email to: support@simcom.com

Version History

Version	Date	Owner	What is new
V2.00	2020.8.6	Yulong.Li	Update the format

Contents

1. Introduction

1.1 Purpose of the document

Based on module AT command manual, this document will introduce SSL application process.

Developers could understand and develop application quickly and efficiently based on this document.

2. SSL Introduction

SSL feature includes SSL (Secure Socket Layer) and TLS (Transport Layer Security). It is used to transport encrypted data based on TCP/IP protocol and SSL/TLS. SSL/TLS usually works between Transport Layer and Application Layer.

2.1 Characteristic

- **Support multiple SSL contexts;**
- **Support encrypted and unencrypted connections;**
  - **Unencrypted Connections**
    Module works as TCP clients. It exchanges unencrypted data with TCP servers by TCP connections.
  - **Encrypted Connections**
    Module works as SSL clients. It exchanges encrypted data with SSL servers by TCP connections.
- **Support multiple data transmission mode;**
  - **Direct Push Mode**
    Host data will be sent to internal protocol stack and forwarded to air interface. Data received from air interface will be transmitted to internal protocol stack and forwarded to COM ports.
  - **Buffer Access Mode**
    Host data will be sent to internal protocol stack and forwarded to air interface. Data received from air interface will be saved into local buffers. Host could retrieve buffer data by AT commands.
  - **Transparent Access Mode**
    Host data will be directly sent to air interface. Data received from air interface will be directly sent to COM ports.

2.2 SSL Context Configuration

Step 1: Configure SSL version by AT+CSSLCFG="sslversion",<ssl_ctx_index>,<sslversion>.

Step 2: Configure SSL authentication mode by AT+CSSLCFG="authmode",<ssl_ctx_index>, <authmode>.

Step 3: Configure the flag of ignore local time by

AT+CSSLCFG="ignorlocaltime",<ssl_ctx_index>,<ignoreltime>.

Step 4: Configure the max time in SSL negotiation stage by

AT+CSSLCFG="negotiatetime",<ssl_ctx_index>,<negotiatetime>.

Step 5: Download the certificate into the module by AT+CCERTDOWN.

Step 6: Configure the server root CA by AT+CSSLCFG="cacert",<ssl_ctx_index>,<ca_file>.

Step 7: Configure the client certificate by AT+CSSLCFG="clientcert",<ssl_ctx_index>,<clientcert_file>.

Step 8: Configure the client key by AT+CSSLCFG="clientkey",<ssl_ctx_index>,<clientkey_file>.

Step 10: Delete the certificate from the module by AT+CCERTDELE.

Step 11: List the certificates by AT+CCERTLIST.

2.3 SSL Commands Process

Step 1: Ensure GPRS network is available before performing SSL related operations.

Step 2: Configure the parameter of PDP context by AT+CGDCONT.

Step 3: Activate the PDP context to start SSL service by AT+CCHSTART.

Step 4: Configure SSL context by AT+CSSLCFG (if connect to SSL/TLS server).

Step 5: Set the SSL context used in SSL connection by AT+CCHSSLCFG (if connect to SSL/TLS server).

Step 6: Connect to the server by AT+CCHOPEN.

Step 7: Send data to the server by AT+CCHSEND.

Step 8: Receive data from server by AT+CCHRECV in manual receive mode.

Step 9: Disconnect from the server by AT+CCHCLOSE.

Step 10: Deactivate the PDP context to stop SSL service by AT+CCHSTOP.

3. AT Commands for SSL

Command	Description
AT+CCHSTART	Start SSL Service
AT+CCHSTOP	Stop SSL Service
AT+CCHOPEN	Setup SSL Client Socket Connections
AT+CCHCLOSE	Destroy SSL Client Socket Connections
AT+CCHSEND	Send SSL Data
AT+CCHRECV	Retrieve SSL Buffer Data
AT+CCHADDR	Get IP Address of PDP Context
AT+CCHSSLCFG	Set SSL Context Index of SSL Connections
AT+CCHCFG	Set Context of SSL Connections
AT+CCHSET	Set Mode of Sending and Receiving SSL Data
AT+CSSLCFG	Configure SSL Context
AT+CCERTDOWN	Download Certificate Files into Module
AT+CCERTDELE	Delete Certificate Files of Module
AT+CCERTLIST	List Certificate Files of Module

For detail information, please refer to “SIM7080 Series_AT Command Manual_V1.00”.

4. Bearer Configuration

Module will usually attach to network and register PS service automatically.

4.1 Start SSL Service

```
//Example of PDN Auto-activation.
AT+CPIN?
+CPIN: READY                          Check Status of SIM Card

OK
AT+CSQ
+CSQ: 27,99                           Check RF Signal

OK
AT+CGREG?
+CGREG: 0,1                           Check Status of PS Service

OK
AT+COPS?
+COPS: 0,0,"CHN-CT",9                 Check Information of Operator

OK
AT+CPSI?
+CPSI:
LTE,Online,460-00,0x1816,27593        Check Information of Network
483,139,EUTRAN-BAND39,38400,
5,5,-88,-868,-578,18

OK
AT+CGDCONT?
+CGDCONT:
1,"IPV4","CMNET","0.0.0.0.0.0.0.      Check Information of PDP Context
0.0.0.0.0.0.0.0",0,0,0,0

OK
```

AT+CGDCONT=1, "IP", "CMNET"	
OK	Set PDP Context
AT+CCHSTART	
OK	
+CCHSTART: 0	Start SSL Service