SIM7500_SIM7600_SIM7800 Series_SSL_Application Note

LTE Module
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

THIS DOCUMENT CONTAINS PROPRIETARY TECHNICAL INFORMATION WHICH IS THE PROPERTY OF SIMCOM WIRELESS SOLUTIONS LIMITED. COPYING, TO OTHERS AND USING THIS DOCUMENT, ARE FORBIDDEN WITHOUT EXPRESS AUTHORITY BY SIMCOM. OFFENDERS ARE LIABLE TO THE PAYMENT OF INDEMNIFICATIONS. ALL RIGHTS RESERVED BY SIMCOM IN THE PROPRIETARY TECHNICAL INFORMATION, INCLUDING BUT NOT LIMITED TO REGISTRATION GRANTING OF A PATENT, A UTILITY MODEL OR DESIGN. ALL SPECIFICATION SUPPLIED HEREIN ARE SUBJECT TO CHANGE WITHOUT NOTICE AT ANY TIME.

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

Copyright © 2020 SIMCom Wireless Solutions Limited All Rights Reserved.
# Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Owner</th>
<th>What is new</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2.00</td>
<td>2020.8.6</td>
<td>Yulong.Li</td>
<td>Update the format</td>
</tr>
</tbody>
</table>
Contents

Version History.................................................................................................................................................... 3

Contents................................................................................................................................................................ 4

1. Introduction................................................................................................................................................... 5
   1.1 Purpose of the document......................................................................................................................... 5

2. SSL Introduction............................................................................................................................................. 6
   2.1 Characteristic........................................................................................................................................... 6
   2.2 SSL Context Configuration....................................................................................................................... 6
   2.3 SSL Commands Process........................................................................................................................... 7

3. AT Commands for SSL................................................................................................................................. 8

4. Bearer Configuration.................................................................................................................................... 9
   4.1 Start SSL Service................................................................................................................................... 9
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="ignor localtime",<ssl_ctx_index>,<ignoretime>.

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

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

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
OK
AT+CSQ
+CSQ: 27,99
OK
AT+CGREG?
+CGREG: 0,1
OK
AT+COPS?
+COPS: 0,0,"CHN-CT",9
OK
AT+CPSI?
+CPSI:
LTE,Online,460-00,0x1816,27593 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.
0.0.0.0.0.0.0.0",0,0,0
OK
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CGDCONT=1, &quot;IP&quot;, &quot;CMNET&quot;</td>
<td>Set PDP Context</td>
</tr>
<tr>
<td>AT+CCHSTART</td>
<td>Start SSL Service</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHSTART: 0</td>
<td></td>
</tr>
</tbody>
</table>