A7600 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
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.
About Document

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Chapter</th>
<th>What is new</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.00</td>
<td>2020.06.19</td>
<td></td>
<td>New version</td>
</tr>
</tbody>
</table>

Scope

This document presents the AT Command Set for SIMCom A7600 Series, including A7600XX-XXXX, A5360E, and A7670X.
Contents

About Document.................................................................................................................... 2
   Version History .................................................................................................................. 2
   Scope ............................................................................................................................... 2

Scope ............................................................................................................................................ 2

Contents ........................................................................................................................................ 3

1 Introduction...................................................................................................................... 4
   1.1 Purpose of the document ............................................................................................ 4
   1.2 Related documents ....................................................................................................... 4
   1.3 Conventions and abbreviations .................................................................................. 4
   1.4 The process of SSL AT Commands .......................................................................... 5
   1.5 Error Handling .......................................................................................................... 6
      1.5.1 Failed to Open SSL Connection .................................................................. 6

2 AT Commands for SSL.................................................................................................... 7

3 SSL Examples .................................................................................................................. 8
   3.1 Access to TCP server ................................................................................................. 8
   3.2 Access to SSL/TLS server (not verify server and client) ......................................... 10
   3.3 Access to SSL/TLS server (only verify the server) .................................................. 12
   3.4 Access to SSL/TLS server (verify server and client) .............................................. 14
   3.5 Access to SSL/TLS server (only verify the client) .................................................. 16
   3.6 Access to SSL/TLS server in transparent mode ...................................................... 18
   3.7 Download certificate into module .......................................................................... 20

4 Appendix ........................................................................................................................ 24
   4.1 Result codes and unsolicited codes ......................................................................... 24
      4.1.1 Command result <err> codes ...................................................................... 24
      4.1.2 Unsolicited result codes .................................................................................. 24
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.

1.2 Related documents


1.3 Conventions and abbreviations

- PDP  Packet Data Protocol;
- SSL  Security Socket Layer;
- URC  Unsolicited result codes;
- DNS  Domain Name Server;
1.4 The process of SSL AT Commands

- **Power on the module**
  - Check the status of SIM card or reboot the module

- **Query SIM card status**
  - AT+CPIN?
  - Check the status of SIM card

- **Query CS service**
  - AT+CREG?
  - CS Service: If <stat> of AT+CREG? equals to 1, it means that the module has registered on CS domain service. Reboot the module if it fails to register on CS domain.

- **Query PS service**
  - AT+CGREG?/AT+CEREG?
  - PS Service: If <stat> of AT+CGREG?/AT+CEREG? equals to 1, it means that the module has registered on PS domain service.

- **Query UE information**
  - AT+CPSI?
  - UE system information: If <System Mode> is "NO SERVICE", it means network status has some problem.

- **Configure the PDP context**
  - AT+CGDCONT=
  1. Configure PDP Context by AT+CGDCONT=<cid>,<PDP_type>,<APN>

- **Active the PDP context**
  - AT+CGACT=<state>,[<cid>]

- **Configure the IP address of the PDP context**
  - AT+CGACT?

- **Configure the PDP context**
  - AT+CGDCONT=

- **Query the IPv4 address after calling AT+CCHSTART**
  - AT+CCHADDR

- **Quit transparent mode**
  - +++

- **Enter transparent mode**
  - ATO

- **Configure the report mode**
  - AT+CCHMODE=0,1? NO
  - AT+CCHMODE=1,1? YES

- **Configure the report mode of sending and receiving data**
  - AT+CCHSET=1,1?

- **Configure the mode of sending and receiving data**
  - AT+CCHMODE=1?
  - If AT+CCHMODE=1 will ignore the AT+CCHSET

- **Start SSL service and active PDP context by AT+CCHSTART**

- **Download certificate into the module**
  - AT+CCERTDOWN=<filename>,<len>

- **Configure the certificate**
  - AT+CCERTCFG

- **Manage and list the certificate**
  - AT+CCERTLIST

- **Configure the SSL context**
  - AT+CCHSSLCFG

- **Connect to the server**
  - AT+CCHOPEN=<session_id>, "host", <port>[<client_type>,[<bind_port>]]

- **Send data directly after showing below words**
  - CONNECT 115200

- **Disconnect from the server**
  - AT+CCHCLOSE=<session_id>

- **Stop SSL service**
  - AT+CCHSTOP

- **Power on the module**
  - Check the status of SIM card or reboot the module

- **Query SIM card status**
  - AT+CPIN?
  - Check the status of SIM card

- **Query CS service**
  - AT+CREG?
  - CS Service: If <stat> of AT+CREG? equals to 1, it means that the module has registered on CS domain service. Reboot the module if it fails to register on CS domain.

- **Query PS service**
  - AT+CGREG?/AT+CEREG?
  - PS Service: If <stat> of AT+CGREG?/AT+CEREG? equals to 1, it means that the module has registered on PS domain service.

- **Query UE information**
  - AT+CPSI?
  - UE system information: If <System Mode> is "NO SERVICE", it means network status has some problem.

- **Configure the PDP context**
  - AT+CGDCONT=
  1. Configure PDP Context by AT+CGDCONT=<cid>,<PDP_type>,<APN>

- **Active the PDP context**
  - AT+CGACT=<state>,[<cid>]

- **Query IP address of the PDP context**
  - AT+CGACT?

- **Configure the mode of sending and receiving data**
  - AT+CCHMODE=1?

- **Configure the report mode**
  - AT+CCHMODE=1?
  - If AT+CCHMODE=1 will ignore the AT+CCHSET

- **Start SSL service and active PDP context by AT+CCHSTART**

- **Download certificate into the module**
  - AT+CCERTDOWN=<filename>,<len>

- **Configure the certificate**
  - AT+CCERTCFG

- **Manage and list the certificate**
  - AT+CCERTLIST

- **Configure the SSL context**
  - AT+CCHSSLCFG
1.5 Error Handling

1.5.1 Failed to Open SSL Connection

If it is failed to open SSL connection, please check the following aspects:
1. Query the status of the specified PDP context by `AT+CGACT?` command to check whether the specified PDP context has been activated.
2. Please check the SSL configuration by `AT+CSSLCFG?` command, especially the SSL version and cipher suite.
3. When the `CCHXXX: <errorcode>` is not 0, it indicates an error code replied from CCH server. For more details, please refer to A7600 Series_AT Command Manual _V1.01.09.
2 AT Commands for SSL

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CSSLCFG</td>
<td>Configure the SSL Context</td>
</tr>
<tr>
<td>AT+CCERTDOWN</td>
<td>Download certificate into the module</td>
</tr>
<tr>
<td>AT+CCERTLIST</td>
<td>List certificates</td>
</tr>
<tr>
<td>AT+CCERTDELE</td>
<td>Delete certificates</td>
</tr>
<tr>
<td>AT+CCHSET</td>
<td>Configure the report mode of sending and receiving data</td>
</tr>
<tr>
<td>AT+CCHMODE</td>
<td>Configure the mode of sending and receiving data</td>
</tr>
<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+CCHADDR</td>
<td>Get the IPv4 address</td>
</tr>
<tr>
<td>AT+CCHSSLCFG</td>
<td>Set the SSL context</td>
</tr>
<tr>
<td>AT+CCHCFG</td>
<td>Configure the Client Context</td>
</tr>
<tr>
<td>AT+CCHOPEN</td>
<td>Connect to server</td>
</tr>
<tr>
<td>AT+CCHCLOSE</td>
<td>Disconnect from server</td>
</tr>
<tr>
<td>AT+CCHSEND</td>
<td>Send data to server</td>
</tr>
<tr>
<td>AT+CCHRECV</td>
<td>Read the cached data that received from the server</td>
</tr>
</tbody>
</table>

For more detailed information, please refer to A7600 Series_AT Command Manual.
3 SSL Examples

Before all SSL related operations, we should ensure the following:
Ensure GPRS network is available:

```
AT+CSQ
+CSQ: 23,0
OK
AT+CREG?
+CREG: 0,1
OK
AT+CGREG?
+CGREG: 0,1
OK
```

3.1 Access to TCP server

Following commands shows how to communicate with a TCP server.

```
AT+CCHSET=1 //Enable reporting +CCHSEND result
OK
AT+CCHSTART
OK
+CCHSTART: 0
AT+CCHOPEN=0,"www.baidu.com",80,1 //connect to TCP server
OK
+CCHOPEN: 0,0
AT+CCHSEND=0,121 //send data to server
>GET / HTTP/1.1
Host: www.baidu.com
User-Agent: Mozilla/5.0 (Windows NT 5.1;
```
rv:2.0) Gecko/20100101 Firefox/4.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie:
BAIDUID=D6F6D0D297C8CAE39BD45C683996696C7:FG=1;
Hm_lvt_9f14aaa038bbba8b12e2a4a3e51d2541321597443439;
USERID=e194072f4759c0f7c2b6e5d3b09298984fd1
OK
+CCHSEND: 0,0
+CCHRECV: DATA,0,757
HTTP/1.1 302 Found
Connection: Keep-Alive
Content-Length: 225
Content-Type: text/html
Date: Wed, 05 Sep 2018 08:59:38 GMT
Location: https://www.baidu.com/
Server: BWS/1.1
Set-Cookie:
BAIDUID=D6F6D0D297C8CAE39BD45C683996696C7; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: PSTM=1536137978; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: BD_LAST_QID=11878059346481009304; path=/; Max-Age=1
X-Ua-Compatible: IE=Edge,chrome=1

<html>
<head><title>302 Found</title></head>
<body bgcolor="white">

//report the received data from server
### 3.2 Access to SSL/TLS server (not verify server and client)

Following commands shows how to access to a SSL/TLS server without verifying the server. It needs to configure the authentication mode to 0, and then it will connect to the server successfully.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CSSLCFG=&quot;sslversion&quot;,0,4</td>
<td>Set the SSL version of the first SSL context</td>
</tr>
<tr>
<td>AT+CSSLCFG=&quot;authmode&quot;,0,0</td>
<td>Set the authentication mode (not verify server) of the first SSL context</td>
</tr>
<tr>
<td>AT+CCHSET=1</td>
<td>Enable reporting +CCHSEND result</td>
</tr>
<tr>
<td>AT+CCHSTART</td>
<td>Start SSL service, activate PDP context</td>
</tr>
<tr>
<td>+CCHSTART: 0</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSSLCFG=0,0</td>
<td>Set the first SSL context to be used in the SSL connection</td>
</tr>
<tr>
<td>AT+CCHOPEN=0, &quot;www.baidu.com&quot;, 443,2</td>
<td>Connect to SSL/TLS server</td>
</tr>
<tr>
<td>+CCHOPEN: 0,0</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSEND=0,121</td>
<td>Send data to server</td>
</tr>
<tr>
<td>&gt;GET / HTTP/1.1</td>
<td></td>
</tr>
</tbody>
</table>
Host: www.baidu.com
User-Agent: MAUI http User Agent
Proxy-Connection: keep-alive
Content-Length: 0

OK
+CCHSEND: 0,0
+CCHRECV: DATA,0,917
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 227
Content-Type: text/html
Date: Tue, 04 Sep 2018 06:21:35 GMT
Etag: "5b7b7f40-e3"
Last-Modified: Tue, 21 Aug 2018 02:56:00 GMT
P3p: CP=" OTI DSP COR IVA OUR IND COM "
Pragma: no-cache
Server: BWS/1.1
Set-Cookie: BD_NOT_HTTPS=1; path=/; Max-Age=300
Set-Cookie: BIDUPSID=D95046B2B3D5455BF01A622DB8DED9EA; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: PSTM=1536042095; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Strict-Transport-Security: max-age=0
X-Ua-Compatible: IE=Edge,chrome=1

<html>
<head>
  <script>
    location.replace(location.href.replace("https://","http://"));
  </script>
</head>
<body>
3.3 Access to SSL/TLS server (only verify the server)

Following commands shows how to access to a SSL/TLS server with verifying the server. It needs to configure the authentication mode to 1 and the right server root CA, and then it will connect to the server successfully.

```
AT+CSSLCFG="sslversion",0,4  //Set the SSL version of the first SSL context
OK

AT+CSSLCFG="authmode",0,1  //Set the authentication mode(verify server) of the first SSL context
OK

AT+CSSLCFG="cacert",0,"ca_cert.pem"  //Set the server root CA of the first SSL context
OK

AT+CCHSET=1  //Enable reporting +CCHSEND result
OK

AT+CCHSTART  // start SSL service, activate PDP context
OK

+CCHSTART: 0

AT+CCHSSLCFG=0,0  // Set the first SSL context to be used in the SSL connection
OK

AT+CCHOPEN=0,"www.baidu.com",443,2  //connect to SSL/TLS server
OK

+CCHOPEN: 0,0

AT+CCHSEND=0,121  //send data to server
```
>GET / HTTP/1.1
Host: www.baidu.com
User-Agent: MAUI htp User Agent
Proxy-Connection: keep-alive
Content-Length: 0

OK

+CCHSEND: 0,0
+CCHRECV: DATA,0,917
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 227
Content-Type: text/html
Date: Tue, 04 Sep 2018 06:21:35 GMT
Etag: "5b7b7f40-e3"
Last-Modified: Tue, 21 Aug 2018 02:56:00 GMT
P3p: CP=" OTI DSP COR IVA OUR IND COM "
Pragma: no-cache
Server: BWS/1.1
Set-Cookie: BD_NOT_HTTPS=1; path=/; Max-Age=300
Set-Cookie: BIDUPSID=D95046B2B3D5455BF01A622DB8DED9EA; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: PSTM=1536042095; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Strict-Transport-Security: max-age=0
X-Ua-Compatible: IE=Edge,chrome=1

<html>
<head>
  <script>
    location.replace(location.href.replace("https:","http://"));
  </script>
</head>
### 3.4 Access to SSL/TLS server (verify server and client)

Following commands shows how to access to a SSL/TLS server with verifying the server and client. It needs to configure the authentication mode to 2, the right server root CA, the right client certificate and key, and then it will connect to the server successfully.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CCHCLOSE=0</td>
<td>//Disconnect from the Service</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSTOP</td>
<td>//stop SSL Service</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSSLCFG=0,0</td>
<td>// Set the first SSL context</td>
</tr>
</tbody>
</table>

AT+CCHCF="sslversion",0,4  
AT+CCHCF="authmode",0,2  
AT+CCHCF="cacert",0,"ca_cert.pem"  
AT+CCHCF="clientcert",0,"cert.pem"  
AT+CCHCF="clientkey",0,"key_cert.pem"  
AT+CCHSET=1                      
AT+CCHSTART                      
AT+CCHSSLCFG=0,0  

//Set the SSL version of the first SSL context

//Set the authentication mode(verify server and client) of the first SSL context

//Set the server root CA of the first SSL context

//Set the client certificate of the first SSL context

//Set the client key of the first SSL context

// Enable reporting +CCHSEND result

// start SSL service, activate PDP context

// Set the first SSL context to be used in the SSL connection
<table>
<thead>
<tr>
<th>Command</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CCHOPEN=0, &quot;www.baidu.com&quot;,443,2</td>
<td>connect to SSL/TLS server</td>
</tr>
<tr>
<td>+CCHOPEN: 0,0</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSEND=0,121</td>
<td>send data to server</td>
</tr>
<tr>
<td>&gt;GET / HTTP/1.1</td>
<td></td>
</tr>
<tr>
<td>Host: <a href="http://www.baidu.com">www.baidu.com</a></td>
<td></td>
</tr>
<tr>
<td>User-Agent: MAUI htp User Agent</td>
<td></td>
</tr>
<tr>
<td>Proxy-Connection: keep-alive</td>
<td></td>
</tr>
<tr>
<td>Content-Length: 0</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHSEND: 0,0</td>
<td></td>
</tr>
<tr>
<td>+CCHRECV: DATA,0,917</td>
<td></td>
</tr>
<tr>
<td>HTTP/1.1 200 OK</td>
<td></td>
</tr>
<tr>
<td>Accept-Ranges: bytes</td>
<td></td>
</tr>
<tr>
<td>Cache-Control: no-cache</td>
<td></td>
</tr>
<tr>
<td>Connection: Keep-Alive</td>
<td></td>
</tr>
<tr>
<td>Content-Length: 227</td>
<td></td>
</tr>
<tr>
<td>Content-Type: text/html</td>
<td></td>
</tr>
<tr>
<td>Date: Tue, 04 Sep 2018 06:21:35 GMT</td>
<td></td>
</tr>
<tr>
<td>Etag: &quot;5b7b7f40-e3&quot;</td>
<td></td>
</tr>
<tr>
<td>Last-Modified: Tue, 21 Aug 2018 02:56:00 GMT</td>
<td></td>
</tr>
<tr>
<td>P3p: CP=&quot; OTI DSP COR IVA OUR IND COM &quot;</td>
<td></td>
</tr>
<tr>
<td>Pragma: no-cache</td>
<td></td>
</tr>
<tr>
<td>Server: BWS/1.1</td>
<td></td>
</tr>
<tr>
<td>Set-Cookie: BD_NOT_HTTPS=1; path=/; Max-Age=300</td>
<td></td>
</tr>
<tr>
<td>Set-Cookie: BIDUPSID=D95046B2B3D5455BF01A622DB8DED9EA; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com</td>
<td></td>
</tr>
<tr>
<td>Set-Cookie: PSTM=1536042095; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com</td>
<td></td>
</tr>
<tr>
<td>Strict-Transport-Security: max-age=0</td>
<td></td>
</tr>
<tr>
<td>X-UA-Compatible: IE=Edge,chrome=1</td>
<td></td>
</tr>
<tr>
<td>&lt;html&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;head&gt;</td>
<td></td>
</tr>
</tbody>
</table>
3.5 Access to SSL/TLS server (only verify the client)

Following commands show how to access to a SSL/TLS server with verifying the client. It needs to configure the authentication mode to 3, the right client certificate and key, and then it will connect to the server successfully.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CCHCLOSE=0</td>
<td>//Disconnect from the Service</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHCLOSE: 0,0</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSTOP</td>
<td>//Stop SSL Service</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHSTOP: 0</td>
<td></td>
</tr>
</tbody>
</table>

//Set the SSL version of the first SSL context
| AT+CSSLCFG="sslversion",0,4                   |                                                                            |
| OK                                           |                                                                             |

//Set the authentication mode (only verify client) of the first SSL context
| AT+CSSLCFG="authmode",0,3                     |                                                                            |
| OK                                           |                                                                             |

//Set the client certificate of the first SSL context
| AT+CSSLCFG="clientcert",0,"cert.pem"          |                                                                            |
| OK                                           |                                                                             |

//Set the client key of the first SSL context
| AT+CSSLCFG="clientkey",0,"key_cert.pem"        |                                                                            |
| OK                                           |                                                                             |

//Enable reporting +CCHSEND result
| AT+CCHSET=1                                   |                                                                            |
| OK                                           |                                                                             |

//Start SSL service, activate PDP context
<p>| AT+CCHSTART                                  |                                                                            |
| OK                                           |                                                                             |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CCHSTART: 0</td>
<td>Set the first SSL context to be used in the SSL connection</td>
</tr>
<tr>
<td>AT+CCHSSLCFG=0,0</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>AT+CCHOPEN=0, &quot;www.baidu.com&quot;, 443,2</td>
<td>Connect to SSL/TLS server</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHOPEN: 0,0</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSEND=0,121</td>
<td>Send data to server</td>
</tr>
<tr>
<td>&gt;GET / HTTP/1.1</td>
<td></td>
</tr>
<tr>
<td>Host: <a href="http://www.baidu.com">www.baidu.com</a></td>
<td></td>
</tr>
<tr>
<td>User-Agent: MAUI htp User Agent</td>
<td></td>
</tr>
<tr>
<td>Proxy-Connection: keep-alive</td>
<td></td>
</tr>
<tr>
<td>Content-Length: 0</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHSEND: 0,0</td>
<td></td>
</tr>
<tr>
<td>+CCHRECV: DATA,0,917</td>
<td></td>
</tr>
<tr>
<td>HTTP/1.1 200 OK</td>
<td></td>
</tr>
<tr>
<td>Accept-Ranges: bytes</td>
<td></td>
</tr>
<tr>
<td>Cache-Control: no-cache</td>
<td></td>
</tr>
<tr>
<td>Connection: Keep-Alive</td>
<td></td>
</tr>
<tr>
<td>Content-Length: 227</td>
<td></td>
</tr>
<tr>
<td>Content-Type: text/html</td>
<td></td>
</tr>
<tr>
<td>Date:Tue, 04 Sep 2018 06:21:35 GMT</td>
<td></td>
</tr>
<tr>
<td>Etag: &quot;5b7b7f40-e3&quot;</td>
<td></td>
</tr>
<tr>
<td>Last-Modified: Tue, 21 Aug 2018 02:56:00 GMT</td>
<td></td>
</tr>
<tr>
<td>P3p: CP=&quot; OTI DSP COR IVA OUR IND COM &quot;</td>
<td></td>
</tr>
<tr>
<td>Pragma: no-cache</td>
<td></td>
</tr>
<tr>
<td>Server: BWS/1.1</td>
<td></td>
</tr>
<tr>
<td>Set-Cookie: BD_NOT_HTTPS=1; path=/; Max-Age=300</td>
<td></td>
</tr>
<tr>
<td>Set-Cookie: BIDUPSID=D95046B2B3D5455BF01A622DB8DED9EA; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com</td>
<td></td>
</tr>
<tr>
<td>Set-Cookie: PSTM=1536042095; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com</td>
<td></td>
</tr>
<tr>
<td>Strict-Transport-Security: max-age=0</td>
<td></td>
</tr>
</tbody>
</table>
3.6 Access to SSL/TLS server in transparent mode

Following commands shows how to access to a SSL/TLS server with not verifying the server in transparent mode. It needs to configure the sending and receiving mode to 1 (the transparent mode). Only the session 0 is support the transparent mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CCHMODE=1</td>
<td>//Set the transparent mode</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSET=1</td>
<td>//Enable reporting +CCHSEND result</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSTART</td>
<td>// start SSL service, activate PDP context</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>+CCHSTART: 0</td>
<td></td>
</tr>
<tr>
<td>AT+CCHSSLCFG=0,0</td>
<td>// Set the first SSL context to be used in the SSL connection</td>
</tr>
</tbody>
</table>
AT+CCHOPEN=0, "www.baidu.com", 443,2
CONNECT 115200
GET / HTTP/1.1
Host: www.baidu.com
User-Agent: MAUI htp User Agent
Proxy-Connection: keep-alive
Content-Length: 0

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 227
Content-Type: text/html
Date: Tue, 04 Sep 2018 06:26:03 GMT
Etag: "5b7b7f40-e3"
Last-Modified: Tue, 21 Aug 2018 02:56:00 GMT
P3p: CP=" OTI DSP COR IVA OUR IND COM "
Pragma: no-cache
Server: BWS/1.1
Set-Cookie: BD_NOT_HTTPS=1; path=/; Max-Age=300
Set-Cookie: BIDUPSID=F19D0F1E532ED84CE275BC100691F9E; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: PSTM=1536042363; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Strict-Transport-Security: max-age=0
X-Ua-Compatible: IE=Edge,chrome=1

<html>
<head>
  <script>
    location.replace(location.href.replace("https:","http:"));
  </script>
</head>
+++ //switch to command mode

OK

AT+CCHCLOSE=0 //Disconnect from the Service

OK

CLOSED

AT+CCHSTOP //stop SSL Service

OK

+CCHSTOP: 0

3.7 Download certificate into module

Following commands shows how to download certificate into module.

AT+CCERTDOWN="client_key.der",1702 //download file with not ASCII coding file name

>-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAlwuz/TNa+foGBG6rXpW
E1Wnuc+GN9vS7MReKOH+z2UfGuaV
BSb8VYFCgoL4RnWLwXAcLlqw88zCN89E
K6lydaAwNml/U6nu3oPsVkn8r9+sOX
yh9VD01DmSU349QJvRgt1ocsF1VTdd6RD
kVtu7FdKv4XC5WHcOD7yrEIsVa7+G
Qbmn5cCCz8E75HH8vHZAOFeaV3HvlHnh/1R
Z+jh4ysyhEmFNOFCn3r9v2yu4kPRX
43xEsB13Ue4HgSbnT+Q7LIEK+dfsMUB0SpS
S2NmQOiqGrmmYygT3/V/IX54hit
gli5bvg9DuNYBwh2C+4nyZF95pMj2dEjf4jN
wlDAQABAolBAAJ9ze06QKDo79p4
3NjfJhck/NTYB0XsIK/+iDhgWt4vogCD6kzG
GxsomU2tdOrsq9x1vXchpeu5lQ
98mrpBhaWNC96JxIOh9O+0q1xNAh8AiH22Q
ZGjUTaC8Jfx+B6w+fbkz37os1/+00
6ZajkbChFTfp7r7ANj5wUEoQKZ4vNpLJxLWD
k6uH4ZMNveWcBaZQ21TUg9ZmosK

-------END RSA PRIVATE KEY-----
EJ2ZER/3kOSBg/2B6F50zyL8f1mbqPahHNLqt
rmdV5/Lr4n74TqZXRwt5C19GrBv
tYXDHc+5Y7e1TUjXv00AMDK+3cVR8m8Oa2
0tSdXjcw2Uk9brxb4uxxreOouGFpW
5I+o+q1ECgYEa4Kkok17DVx5FlapFQvJ2Jqi2/
WhzDncuBgbZtcLZnwRFkPn3cBZ
JGNwxyYfEdwtPtVYQYh6Qgq81XRdSRff43G
zkQNmkP0dZM0x3tFwzV6K5Fg7aeR
g5OuddaA9MraCItGqK++7C6BvA3lmXciK4V
WeSZOMDW99Y6mgf92RdkCGYEArB2u
/ltd27LQGBmx0Z+36Hfdixo6RQ+dB+m6XBm
R8iuB/jGO/5PhdFoKoF2qa9Yj2W1+x
B29Xmc1HS6GtvDsN5JXNO7fDmlAxd5whb
wDdcmV3Vet8xJzUeAClawjKtVcFoH
LrNiLdBttWVviCZg+9HhvPuPm14oOfN/Xt
48CgYACxDJ66thUDpsy6mDoGOfi5
kaRHNi00JYuMhFOz+EVDvwLqfhh2RzneKiiu
U8/1oVb+G4e7zx6FxxMwsbEgYEmQ
hmomo0Kn3qPhMNHanvr572Ou7KM2p5hF4
MT/GM0IHdU31D1JrTcJap1TvomAaCL
FqY88arQFWFSz8Hfle0r6QKBgCbQLTtdzKzq
Jdt8+6cwQFYg+9O59MjGVeNfsks
chhzVFAX0n9Tl5Lq9fMJ5FX4g+3JGargjfWuG
CTTFBk0TM2t4wde7AmwiiviV5LU
T2Af06pLTKrS9E9k+yX2Iug+O156VfsbleAm/N
9g5RCJ91CJvFgULro6/axNmnWORf
9kT7AoGBALK4edrX1MjrerCsLu3y9Dy4pAx6E
R6e4xpk025U8wUcqqc+YD2m2xIA
DjqROIzexXkmPlyRKAxyrhh8LmXT/0OFU
APsTqUZ9LBvqiIM+G2OFpbdKDwe
ZBNAgwFpFIUvO0YnZF8rBq0tepqvrayEWd
KKfMMJjq+I72SxD
-----END RSA PRIVATE KEY-----
OK
AT+CCERTDOWN={non-ascii}"262378344532
443B26237835334453B2E70656D",1918
>-----BEGIN CERTIFICATE-----
MIIFCDAYyGQwBAGgIBAzIzPau7FelQswDQY
JKoZIhvcNADELBQAwQDELMakGA1UE
BhMCU0kxGzA8BGvNVBAoMEhN0YXRIWLuC
3RpdHvoaW9uczEUMBGA1UEAxwLVGF4
IENBIFRIc3QwHhcNMTUwNzIzMTUyOTA1Wh
cMNzUwNzIzMTUyOTA1WjBAMQswCQYD
VQQGeAovJSTSeBMkBGA1UECgwSc3RhdGUt
aW5zdGl0dXRpb25zMRQwEgYDVQQDTCDATU
YXggQ0ExVGVzdDCAlwDQYJKoZIhvcNAQ
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CCERTLIST</td>
<td>List certificate files</td>
</tr>
</tbody>
</table>
+CCERTLIST: "中华.pem" |                                                   |
+CCERTLIST: "client_key.der" |                                                   |
| OK              |                                                  |
4 Appendix

4.1 Result codes and unsolicited codes

4.1.1 Command result <err> codes

<table>
<thead>
<tr>
<th>Result codes</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Operation succeeded</td>
</tr>
<tr>
<td>1</td>
<td>Alerting state(reserved)</td>
</tr>
<tr>
<td>2</td>
<td>Unknown error</td>
</tr>
<tr>
<td>3</td>
<td>Busy</td>
</tr>
<tr>
<td>4</td>
<td>Peer closed</td>
</tr>
<tr>
<td>5</td>
<td>Operation timeout</td>
</tr>
<tr>
<td>6</td>
<td>Transfer failed</td>
</tr>
<tr>
<td>7</td>
<td>Memory error</td>
</tr>
<tr>
<td>8</td>
<td>Invalid parameter</td>
</tr>
<tr>
<td>9</td>
<td>Network error</td>
</tr>
<tr>
<td>10</td>
<td>Open session error</td>
</tr>
<tr>
<td>11</td>
<td>State error</td>
</tr>
<tr>
<td>12</td>
<td>Create socket error</td>
</tr>
<tr>
<td>13</td>
<td>Get DNS error</td>
</tr>
<tr>
<td>14</td>
<td>Connect socket error</td>
</tr>
<tr>
<td>15</td>
<td>Handshake error</td>
</tr>
<tr>
<td>16</td>
<td>Close socket error</td>
</tr>
<tr>
<td>17</td>
<td>Nonet</td>
</tr>
<tr>
<td>18</td>
<td>Send data timeout</td>
</tr>
<tr>
<td>19</td>
<td>Not set certificates</td>
</tr>
</tbody>
</table>

4.1.2 Unsolicited result codes

<table>
<thead>
<tr>
<th>Unsolicited codes</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>+CCHEVENT: &lt;session_id&gt;,RECV EVENT</td>
<td>In manual receiving mode, when new data of a</td>
</tr>
</tbody>
</table>
connection arriving to the module, this unsolicited result code will be reported to MCU.

| +CCH_RECV_CLOSED: <session_id>,<err> | When receive data occurred any error, this unsolicited result code will be reported to MCU. |
| +CCH_PEER_CLOSED: <session_id> | The connection is closed by the server. |