A76XX 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
SIMCom Headquarters Building, Building 3, No. 289 Linhong 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 © 2021 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>
<tr>
<td>V1.01</td>
<td>2021.07.02</td>
<td>All</td>
<td>Add support on A7678 Series</td>
</tr>
<tr>
<td>V1.02</td>
<td>2021.11.08</td>
<td>Scope</td>
<td>Scope description is updated</td>
</tr>
</tbody>
</table>
Scope

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. This document applies to A1803S Series, A1603 Series, A1601 Series and A1802 Series.
Contents

About Document.................................................................................................................................................. 2
  Version History................................................................................................................................................. 2
  Scope................................................................................................................................................................ 3

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

1  Introduction......................................................................................................................................................... 5
  1.1 Purpose of the document.......................................................................................................................... 5
  1.2 Related documents........................................................................................................................................ 5
  1.3 Conventions and abbreviations.................................................................................................................. 5
  1.4 The process of SSL AT Commands.......................................................................................................... 6
  1.5 Error Handling............................................................................................................................................. 7
    1.5.1 Failed to Open SSL Connection......................................................................................................... 7

2  AT Commands for SSL........................................................................................................................................ 8

3  SSL Examples...................................................................................................................................................... 9
  3.1 Access to TCP server................................................................................................................................. 9
  3.2 Access to SSL/TLS server (not verify server and client).......................................................................... 11
  3.3 Access to SSL/TLS server (only verify the server)................................................................................... 13
  3.4 Access to SSL/TLS server (verify server and client)................................................................................ 15
  3.5 Access to SSL/TLS server (only verify the client).................................................................................... 17
  3.6 Access to SSL/TLS server in transparent mode....................................................................................... 19
  3.7 Download certificate into module............................................................................................................ 21

4  Appendix.......................................................................................................................................................... 25
  4.1 Result codes and unsolicited codes........................................................................................................ 25
    4.1.1 Command result <err> codes............................................................................................................. 25
    4.1.2 Unsolicited result codes...................................................................................................................... 25
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
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 A76XXSeries_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 *A76XXSeries_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=D6F6D0D297CCAE39BD45C683996696C7:FG=1;
Hm_lvt_9f14aaa038bbba8b12ec2a4a3e51d254=1321597443439;
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:
BIDUPSID=D6F6D0D297CCAE39BD45C683996696C7; 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">
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.

```
AT+CSSLCFG="sslversion",0,4 //Set the SSL version of the first SSL context
OK
AT+CSSLCFG="authmode",0,0 //Set the authentication mode(not verify server) 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>
<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
// start SSL service, activate PDP context
AT+CCHSTART
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 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=D95046B2B3D5455BF01A622DB8D9EA; 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.

```
AT+CSSLCFG="sslversion",0,4  //Set the SSL version of the first SSL context
OK
AT+CSSLCFG="authmode",0,2  //Set the authentication mode(verify server and client) 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+CSSLCFG="clientcert",0,"cert.pem"  //Set the client certificate of the first SSL context
OK
AT+CSSLCFG="clientkey",0,"key_cert.pem"  //Set the client key 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

+CHCOPEN: 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

+CHSENM: 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=D95046B3B3D5455BF01A622DB8DED9EA; 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>
//report the received data from server
</head>
3.5 Access to SSL/TLS server (only verify the client)

Following commands shows 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.

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

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

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

AT+CSSLCFG="clientkey",0,"key_cert.pem" //Set the client key 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 ht p 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

// report the received data from server
X-Ua-Compatible: IE=Edge,chrome=1

<html>
<head>
  <script>
    location.replace(location.href.replace("https:","http://"));
  </script>
</head>
<body>
  <noscript>
    <meta http-equiv="refresh" content="0;url=http://www.baidu.com/"/>
  </noscript>
</body>
</html>

AT+CCHCLOSE=0  //Disconnect from the Service
OK

+CCHCLOSE: 0,0

AT+CCHSTOP  //stop SSL Service
OK

+CCHSTOP: 0

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.

AT+CCHMODE=1  //Set the transparent mode
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
CONNECT 115200
GET / HTTP/1.1
Host: www.baidu.com
User-Agent: MAUI htp User Agent
Proxy-Connection: keep-alive  //send data to server
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=F19D0F1E532ED84CE275BC1006F91F9E; 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.

```plaintext
AT+CCERTDOWN="client_key.der",1702 //download file with not ASCII coding file name
>-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAlwuz/TNa+foGBG6rXpW
E1Wnuc+GN9vS7MRenKOH+z2UfGuaV
BSb8VYFCgoL4RnWLwXAcL1aqw8zCN89E
K6lydaAwNm/U6nu3oPsVkn8r9+sOX
yh9V01DmSU349QWJvRgt1ocsFl1VTdd6RD
kVtu7FdKv4XC5WHcOD7yrEl5Va7+G
Qbnm5cCCz8E75H8vHZAOFeaV3HvlHnh/1R
Z+jh4ysyhEmFNOFCn3r9v2yu4kPRX
43xBsB13Ue4HgSbnT+Q7LIEK+dfsnuBosps
S2NAmQQiGGrmmYygT3/VlISX54hit
gii5bvg9DuNHYBwh2C+4nyZF95pMj2dEJf4jN
wIDAQABAOlBAAJ9ze06QKDo79p4
3NhjJhck/NTYB0XsIK/+iDhgWt4VolgCD6kzG
GxsomU2tdOrsq9x1vXcthepu5lQ
98mrpBhaWNC96JxIOh9O+0q1xNAh8AiH22Q
ZGjUTaC8Jfxt+B6w+fbkz37os1/00
6ZajkbChFTfp7r7ANj5wUEoQKZ4vNpLJxLWD
k6uH4ZMNvWcBaZQ21TUp9ZmoskK
-----END RSA PRIVATE KEY-----
```
OK

AT+CERTDOWN={non-ascii}"262378344352443B262378353334435B2E70656D",1918

//download file with ASCII coding file name
5cVhxUkaEShdx4bjgvKB7JRF2T2
ST1lrKEM2DY=
-----END CERTIFICATE-----
OK
AT+CCERTLIST //list certificate files
+CCERTLIST: "&#x4E2D;&#x534E::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>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>+CCH_RECV_CLOSED: &lt;session_id&gt;,&lt;err&gt;</td>
<td>When receive data occurred any error, this unsolicited result code will be reported to MCU.</td>
</tr>
<tr>
<td>+CCH_PEER_CLOSED: &lt;session_id&gt;</td>
<td>The connection is closed by the server.</td>
</tr>
</tbody>
</table>

connection arriving to the module, this unsolicited result code will be reported to MCU.