A76XX Series_ SSL_Application Note

LTE Module

Document Title:	A76XX Series_SSL_Application Note
Version:	1.03
Date:	2022.05.20
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

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 © 2022 SIMCom Wireless Solutions Limited All Rights Reserved.

About Document

Version History

Version	Date	Owner	What is new
V1.00	2020.06.19	Zheng.huang	New version
V1.01	2021.02.03	Zheng.huang	Add support on A7678 Series
V1.02	2021.11.25	Zheng.huang	Adjust example fomat
V1.03	2022.05.20	Chunyan.yang	Perpared for the archives

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

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] A76XXSeries_AT Command Manual

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
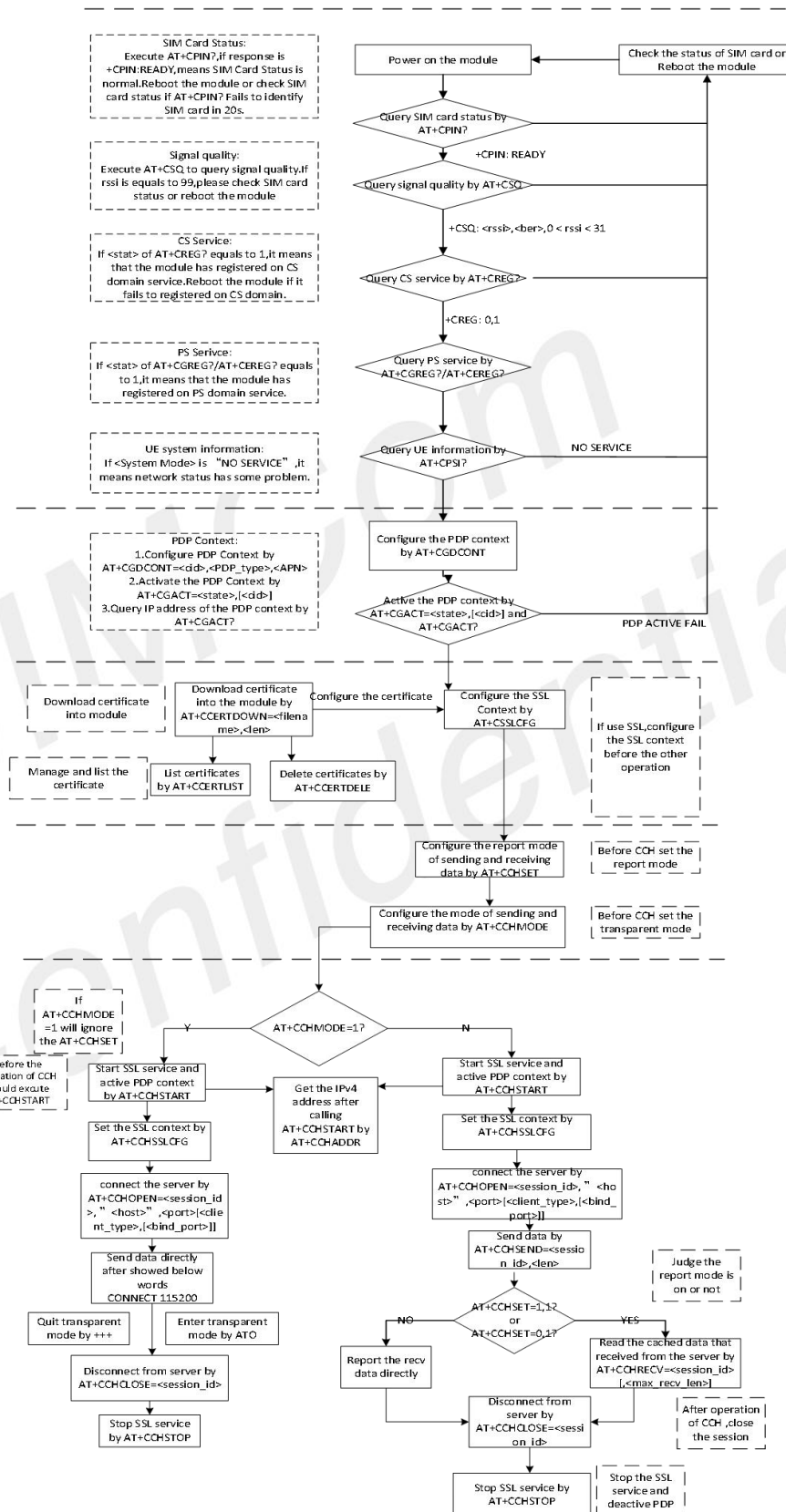
1.5 Error Handling

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 A76XX Series_AT Command Manual.

2 AT Commands for SSL

Command	Description
AT+CSSLCFG	Configure the SSL Context
AT+CCERTDOWN	Download certificate into the module
AT+CCERTLIST	List certificates
AT+CCERTDELE	Delete certificates
AT+CCHSET	Configure the report mode of sending and receiving data
AT+CCHMODE	Configure the mode of sending and receiving data
AT+CCHSTART	Start SSL service
AT+CCHSTOP	Stop SSL service
AT+CCHADDR	Get the IPv4 address
AT+CCHSSLCFG	Set the SSL context
AT+CCHCFG	Configure the Client Context
AT+CCHOPEN	Connect to server
AT+CCHCLOSE	Disconnect from server
AT+CCHSEND	Send data to server
AT+CCHRECV	Read the cached data that received from the server

For more detailed information, please refer to A76XX 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=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   //report the received data from server

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">

```
<center><h1>302 Found</h1></center>
<hr><center>7a367f7b87705e16b985e34ca59
b8ae8b1d28d47
Time : Tue Aug 21 10:55:16 CST
2018</center>
</body>
</html>
```
AT+CCHCLOSE=0   //Disconnect from the Service

OK

+CCHCLOSE: 0,0
AT+CCHSTOP   //stop SSL Service
OK

+CCHSTOP: 0

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=D95046B2B3D5455BF01A622DB8
DED9EA; expires=Thu, 31-Dec-37 23:55:55   //report the received data from server
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("ht**
tps://","http://"));
**   </script>**
</head>
<body>

```
    <noscript><meta    http-equiv="refresh"
content="0;url=http://www.baidu.com/"></nos
cript>
</body>
</html>
```
AT+CCHCLOSE=0   //Disconnect from the Service

OK

+CCHCLOSE: 0,0

AT+CCHSTOP   //stop SSL Service

OK

+CCHSTOP: 0

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 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=D95046B2B3D5455BF01A622DB8
DED9EA; expires=Thu, 31-Dec-37 23:55:55      //report the received data from server
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("ht
tps://","http://"));
    </script>
</head>
```

```
<body>
    <noscript><meta      http-equiv="refresh"
content="0;url=http://www.baidu.com/"></nos
cript>
</body>
</html>
AT+CCHCLOSE=0                              //Disconnect from the Service
OK


+CCHCLOSE: 0,0
AT+CCHSTOP                                 //stop SSL Service
OK


+CCHSTOP: 0
```

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
                                      //Set the first SSL context to be used in the SSL
AT+CCHSSLCFG=0,0                      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=/;   //report the received data from server

Max-Age=300

Set-Cookie: BIDUPSID=D95046B2B3D5455BF01A622DB8 DED9EA; 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("ht
tps://","http://"));
    </script>
</head>
<body>
    <noscript><meta     http-equiv="refresh"
content="0;url=http://www.baidu.com/"></nos
cript>
</body>
</html>
```

AT+CCHCLOSE=0   //Disconnect from the Service

OK

+CCHCLOSE: 0,0

AT+CCHSTOP   //stop SSL Service

OK

+CCHSTOP: 0

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 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   //report the received data from server
Set-Cookie: BD_NOT_HTTPS=1;   path=/;
Max-Age=300
Set-Cookie:
BIDUPSID=D95046B2B3D5455BF01A622DB8
DED9EA; 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("ht
tps://","http://"));
    </script>
</head>
<body>
    <noscript><meta       http-equiv="refresh"
content="0;url=http://www.baidu.com/"></nos
cript>
</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; //report the received data from server

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("ht tps://","http://"));

</script>

</head>

```
<body>
    <noscript><meta       http-equiv="refresh"
content="0;url=http://www.baidu.com/"></nos
cript>
</body>
</html>
+++                                          //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 >-----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEAIwuz/TNa+foGBG6rXpW E1Wnuc+GN9vS7MRenKOH+z2UfGuaV BSb8VYFCgoL4RnWLwXAcLIaqw88zICN89E K6IydaAwNmI/U6nu3oPsVkn8r9+sOX yh9VD01DmSU349QWJvRgt1ocsFI1VTdd6RD kVtu7FdKv4XC5WHcOD7yrEIsVa7+G Qbnm5cCCz8E75HH8vHZAOFeaV3HvIHnh/1R Z+jh4ysyhEmFNOFCn3r9v2yu4kPRX 43xEsB13Ue4HgSbnT+Q7LIEK+dfsmUBoSps S2NAmQOiqGrmmYygT3/V/ISX54hit gli5bvg9DuNHYBwh2C+4nyZF95pMj2dEJf4jN wIDAQABAoIBAAJ9ze06QKDo79p4 3NjFjJhck/NTYB0XsIK/+iDhgWt4VogCD6kzG GxsomU2tdOrsq9xIvXcthpeu5IQ 98mrpBhaWNC96JxIOh9O+0q1xNAh8AiH22Q ZGjUTaC8Jfx+B6w+fbkz37os1/+00 6ZajkbChFTfp7r7ANj5wUEoQKZ4vNpLJxLWD k6uH4ZMNveWcBaZQ21TUg9ZmoskK	//download file with not ASCII coding file name

EJ2ZEr/3kOSBgi2B6F50zyL8f1mbqPahHNLqt
rndV5/Lr4n74TqZXRwt5Cl9GrBv
tYXDHc+5Y7e1TUIXV00AMDlk+3cVR8m8Oa2
0tSdXjcw2iUk9brxb4uxreOouGfPW
5lO+q1ECgYEA4Kkok17DVx5FiapFQvJ2Jqi2/
WhzDncuBGbZtcLZnwRVfkPn3cBZ
JGNwxYyfEdwltPvTYQYh6Qg81XRdSRfF43G
zkQXNmkPOdZM0x3tFwzV6K5Fg7aeR
g50UddaA9MraCltOgK++7C6BvA3lmXciK4V
WeSZOmDW99Y6mgf92RdkCgYEArB2u
/ld72LGQBmx0Z+36Hf1dxo6RQ+dB+m6XBM
R8iuB/jGO/5PHdFoKoF2qa9Yj2W1+X
B29Xmc1HS6GTvkDlsN5JXNO7fDmlAxd5whb
wDdcmv3VEt8xJ2UeAClawjKtVcFoH
LRNlvDBttWVvlCZg+9HfVpuPm14oFxN/HtSXt
48CgYACxDJ6thUDspy6mD0oGOl5
kaRHNl0OJYuMhFOz+EVDvwLqfh2RzneKiiru
U8/1oVb+G4e7zx6FxxMwsbEgYEmQ
hmrmo0Kn3qPhMMHanvr572Oku7KM2p5hF4
MT/GM0lHdU31D1JrTcJap1TVomAaCL
FqY88arQFwFSz8Hfle0r6QKBgCbQLtTdzKzq
Jdt8+6cwQFYg+9O59MJGVVefNskp
chhzVfAX0n9Tl5Lq9fMJ5FX4g+3JGargjfWuG
CTTFBk0TM2t4wde7AmwiiivU5LU
T2Afo6pLTKrSE9k+yX2iug+O156VfsbleAm/N
g5RCJ91JCvFgULro6/axNmnWORf
9rK7AoGBAlK4edrX1MjerCsLu3y9Dy4pAx6E
R6ei4xpkO25U8wUcqqc+YD2m2xlA
DjqROlTeaxXkmPlyRKAXVarhk8LmXT/oDFU
APsTqUZ9LBrviqtMi+G2OFPbdKDwe
ZBNAgwFpFlUVoi0UYnZF8rBq0tepqivrayEWd
KKfMMJjq+l72SxD
-----END RSA PRIVATE KEY-----
OK
**AT+CCERTDOWN={non-ascii}"262378344532
443B262378353334453B2E70656D",1918**
>-----BEGIN CERTIFICATE-----
MIIFRDCCAyygAwIBAgIIZmPau7FelQswDQY
JKoZlhvcNAQELBQAwQDELMAkGA1UE
BhMCU0kxGzAZBgNVBAoMEnN0YXRlLWluc
3RpdHV0aW9uczEUMBIGA1UEAwwLVGF4
IENBIFRlc3QwHhcNMTUwNzIzMTUyOTA1Wh
cNMzUwNzIzMTUyOTA1WjBAMQswCQYD
VQQGEwJTSTEbMBkGA1UECgwSc3RhdGUt
aW5zdGl0dXRpb25zMRQwEgYDVQQDDAtU
YXggQ0EgVGVzdDCCAilwDQYJKoZlhvcNAQ

//download file with ASCII coding file name

EBBQADgglPADCCAgoCgglBALmH3XNA
KDgN8+G2jX4W/a7LTER10VbRhkGeuc9zyOuj
9gigYXLno4lm/S4iXMcCs1lxgSsj
NJ1YMOje4qgHbFKQwWV588VDw7/fiMMZIXv
FjHfladdHASEDMT53bKX3HIdJZ/iL
6xhpJ/+C/l8dnWcMZUkeP+9BUAni/l2xrHaAVll
i0aS6uc/DjO7b4Gj1Vl4FGlHo
DIH+LmWz26P2gg2xnpWglxXzs5sN8nYErwu
+6h/9xREHco8PPCAZb5HZhqolzYzk
N1S1Do6qAzt/wJM0mhWOWHt9fhp/RoYQ5ZF
ClZmgd1cJcr6S6U7ebAQ+yYRslWU5
+FLYZ4Zlt3ZAHNWyraMee/kFsaGcO21cwE+t
PDOln41B8XvfaXApQt4+TejZWzoH
V0ojA+9H8V+wCFVMJssViFOzuS6SlEZ/xzslo
+B//cfUkq/PnWLJHEy4BJXsj4+F
CvliZ7Lq3B/RcQmBjmTRQ0mxahiMGrrQW4T
LjUYgY8lfwKfMfwFwVwUyk5br9Grs
UX7jy7+Xx17Qed4p0jjOC7KutzRlGr6ULSk11q
pd5lHelwzSOaTXk6rAzZYupPH5
KvY65mdRfq0C0cB2bMvk9m9lyeLfZz5+L9XD
LlodTdwOeWaKvjFErT8WSEkpHxtG
q13TVgicoxsHC2K+8hpFjpaz69ZCmTzj4/17A
gMBAAGjQjBAMB0GA1UdDgQWBBQz
zVr7CUfHAeY2KCb1gXy3jjX3sjAPBgNVHRM
BAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwlBBjANBgkqhkiG9w0BAQsFAAOCAgEAR
9xtbaNa/jSAAyqe3aq88GG7rCyxROGH
BPcakfMmhx1cLYdcY5ATXL/n67eo+S+1g7e/s
K3fVXav5qWs9oUEhAOgcOACMohu
JlBbMq2Qp8lxdpiRWCcyiY1vGQcHcZ02oey/c
06fBZE4iqJdYAhYhsBB5H+idtwJ
s6Lade4wqG58hWCNKBxU+KWDckGGX5Cxs
fU7gdYgjyKq0ow60qQWi4H8pD+WO1Bn
rvlSkAT7vMk2BOz+YlCKZmuq0h3PCkK5T6x
A01fUZCaeze0RozFaekDBEHK0bc1D
My3SKbB3cjdcMzmV8sVdxnNOTxlrP7+Binct
xT3q3Va96kTmwl5pD0x6KOwC7Urr
53ubhl3U2XBAzkk14lDLU+7tqBqhDWwlMN0
NyW1MRTF8JB9Rz+4yCcDWMOT/FZg7
C60RrcnaO/0GETDz6Xl6zedBXo1Q/rJTtXMOr
8iVnc+joZyO2lmOuTwP3C7M3Bnp
gFHqDtD48n9PV9prhbD4fYPyMe/3rshtBcpGA
y2cGjpsP28pkvP8lwBaP8pnpxvQ
7d3oiCBzznaOHjhm8+8C53b/1txzj/LP/4Zzlyns
Ohxy4cihEPhAg1MKUY9qnbw9
9Q6EKrCSqk3TPqiWrTtu4pxyiEiquCHk8n+HX

5cVhxUkaEShdx4bjgvKB7JRF2T2
ST1lrKEM2DY=
-----END CERTIFICATE-----
OK
AT+CCERTLIST   //list certificate files
+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

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

4.1.2 Unsolicited result codes

Unsolicited codes	Meaning
+CCHEVENT: <session_id>,RECV EVENT	In manual receiving mode, when new data of a

	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.