SIM82XX_SIM83XX Series _SSL_Application Note

5G Module

SIMCom Wireless Solutions Limited
SIMCom Headquarters Building, Building 3, No. 289
Linhong Road, Changning District, Shanghai P.R. China
Tel: 86-21-31575100
support@simcom.com
www.simcom.com

Document Title:	SIM82XX_SIM83XX Series_SSL_Application Note
Version:	1.01
Date:	2021.11.25
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
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

About Document

Version History

Version	Date	Owner	What is new
V1.00	2020.8.17	Yulong.Li	First Release
V1.01	2021.11.25	Xianxiang.Ma	Update the format

Scope

This document applies to the SIMCom SIM820X series, SIM821X series, SIM826X series and SIM83XX 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] SIM82XX_SIM83XX Series_AT Command Manual

1.3 Conventions and abbreviations

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 protocol. 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 9: Delete the certificate from the module by AT+CCERTDELE.

Step 10: 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 " SIM82XX_SIM83XX Series_AT Command Manual".

4 Bearer Configuration

Make sure that the module has been attached to network and APN has been configured before starting SSL service.

```
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+CEREG?
+CEREG: 0,1

OK
AT+CPSI?
+CPSI:
LTE,Online,460-00,0x1816,27593490,295,EUTR
AN-BAND3,1300,5,5,-98,-738,-440,8
+CPSI:
NR5G_NSA,210,NR5G_BAND41,504990,-1000,-     // Check Information of Network
140,55

OK
AT+CGDCONT=1, "IP", "CMNET"                     // Set PDP Context Information
OK
AT+CGDCONT?
+CGDCONT:
1,"IPV4","CMNET","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0     // Check Information of PDP Context

OK
```

5 SSL Examples

5.1 Access to TCP server

Following commands shows how to communicate with a TCP server.

```
AT+CCHSET=1                                   // Enable reporting +CCHSEND result
OK
AT+CCHSTART                                   // start SSL service, activate PDP context
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:F
G=1;
Hm_lvt_9f14aaa038bbba8b12ec2a4a3e51d254=1321597
443439;
USERID=e194072f4759c0f7c2b6e5d3b09298984fd1
OK

+CCHSEND: 0,0
+CCHRECV: DATA,0,757                          // report the received data from server
```

```
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">
<center><h1>302 Found</h1></center>
<hr><center>7a367f7b87705e16b985e34ca59b8ae8b1
d28d47
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
```

5.2 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                         // report the received data from server
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=D95046B2B3D5455BF01A622DB8DED
9EA; 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>
    <noscript><meta http-equiv="refresh"
content="0;url=http://www.baidu.com/"></noscrip
t>
</body>
</html>
AT+CCHCLOSE=0                          // Disconnect from the Service
OK

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

+CCHSTOP: 0
```

5.3 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                         // report the received data from server
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=D95046B2B3D5455BF01A622DB8DE
D9EA; 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>
    <noscript><meta http-equiv="refresh"
content="0;url=http://www.baidu.com/"></noscri
pt>
</body>
</html>
AT+CCHCLOSE=0                          // Disconnect from the Service
OK

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

+CCHSTOP: 0
```

5.4 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

+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                         // report the received data from server
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=D95046B2B3D5455BF01A622DB8DE
D9EA; 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>
    <noscript><meta http-equiv="refresh"
content="0;url=http://www.baidu.com/"></noscri
pt>
</body>
</html>
AT+CCHCLOSE=0                          // Disconnect from the Service
OK

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

+CCHSTOP: 0
```

5.5 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                    // report the received data from server
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=D95046B2B3D5455BF01A622DB8DE
D9EA; 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>
    <noscript><meta http-equiv="refresh"
content="0;url=http://www.baidu.com/"></noscri
pt>
</body>
</html>
AT+CCHCLOSE=0                           // Disconnect from the Service
OK
```

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

+CCHSTOP: 0
```

5.6 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                         // report the received data from server
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=F19D0F1E532ED84CE275BC1006F91
F9E; 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>
<body>
    <noscript><meta http-equiv="refresh"
content="0;url=http://www.baidu.com/"></noscri
pt>
</body>
</html>
+++                                          // switch to command mode
OK
AT+CCHCLOSE=0                                // Disconnect from the Service
OK

CLOSED
AT+CCHSTOP                                   // stop SSL Service
OK

+CCHSTOP: 0
```

5.7 Download certificate into module

Following commands shows how to download certificate into module.

```
AT+CCERTDOWN="client_key.der",1702                    // download file with ASCII coding file name
> -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAlwuz/TNa+foGBG6rXpWE1Wnuc+
GN9vS7MRenKOH+z2UfGuaV
BSb8VYFCgoL4RnWLwXAcLlaqw88zlCN89EK6IydaAw
NmI/U6nu3oPsVkn8r9+sOX
yh9VD01DmSU349QWJvRgt1ocsFI1VTdd6RDkVtu7Fd
Kv4XC5WHcOD7yrEIsVa7+G
Qbnm5cCCz8E75HH8vHZAOFeaV3HvIHnh/1RZ+jh4ys
yhEmFNOFCn3r9v2yu4kPRX
43xEsB13Ue4HgSbnT+Q7LlEK+dfsmUBoSpsS2NAmQ
OiqGrmmYygT3/V/lSX54hit
gli5bvg9DuNHYBwh2C+4nyZF95pMj2dEJf4jNwIDAQAB
AoIBAAJ9ze06QKDo79p4
3NjFjJhck/NTYB0XslK/+iDhgWt4VogCD6kzGGxsomU2t
dOrsq9xlvXcthpeu5IQ
98mrpBhaWNC96JxlOh9O+0q1xNAh8AiH22QZGjUTaC
8Jfx+B6w+fbkz37os1/+00
6ZajkbChFTfp7r7ANj5wUEoQKZ4vNpLJxLWDk6uH4ZM
NveWcBaZQ21TUg9ZmoskK
EJ2ZEr/3kOSBgi2B6F50zyL8f1mbqPahHNLqtrndV5/Lr4
n74TqZXRwt5Cl9GrBv
tYXDHc+5Y7e1TUlXV00AMDIk+3cVR8m8Oa20tSdXjcw
2iUk9brxb4uxreOouGfPW
5lO+q1ECgYEA4Kkok17DVx5FiapFQvJ2Jqi2/WhzDncu
BGbZtcLZnwRVfkPn3cBZ
JGNwxYyfEdwltPvTYQYh6Qg81XRdSRfF43GzkQXNm
kPOdZM0x3tFwzV6K5Fg7aeR
g50UddaA9MraCltOgK++7C6BvA3ImXciK4VWeSZOmD
W99Y6mgf92RdkCgYEArB2u
/Id72LGQBmx0Z+36Hf1dxo6RQ+dB+m6XBMR8iuB/jG
O/5PHdFoKoF2qa9Yj2W1+X
B29Xmc1HS6GTvkDIsN5JXNO7fDmlAxd5whbwDdcmv
3VEt8xJ2UeACIawjKtVcFoH
LRNlvDBttWVvlCZg+9HfVpuPm14oFxN/HtSXt48CgYA
CxDJ6thUDspy6mD0oGOI5
kaRHNI0OJYuMhFOz+EVDvwLqfh2RzneKiiruU8/1oVb+
G4e7zx6FxxMwsbEgYEmQ
hmrmo0Kn3qPhMMHanvr572Oku7KM2p5hF4MT/GM0I
HdU31D1JrTcJap1TVomAaCL
```

```
FqY88arQFwFSz8Hfle0r6QKBgCbQLtTdzKzqJdt8+6cw
QFYg+9O59MJGVVefNskp
chhzVfAX0n9Tl5Lq9fMJ5FX4g+3JGargjfWuGCTTFBk0
TM2t4wde7AmwiiivU5LU
T2Afo6pLTKrSE9k+yX2iug+O156VfsbIeAm/Ng5RCJ91J
CvFgULro6/axNmnWORf
9rK7AoGBAIK4edrX1MjerCsLu3y9Dy4pAx6ER6ei4xpk
O25U8wUcqqc+YD2m2xlA
DjqROITeaxXkmPIyRKAXVarhk8LmXT/oDFUAPsTqUZ
9LBrviqtMi+G2OFPbdKDwe
ZBNAgwFpFlUVoi0UYnZF8rBq0tepqivrayEWdKKfMMJj
q+l72SxD
-----END RSA PRIVATE KEY-----
OK
AT+CCERTDOWN={non-ascii}"262378344532443B26    // download file with not ASCII coding file
2378353334453B2E70656D",1918                   // name
>-----BEGIN CERTIFICATE-----
MIIFRDCCAyygAwIBAgIIZmPau7FeIQswDQYJKoZIhvc
NAQELBQAwQDELMAkGA1UE
BhMCU0kxGzAZBgNVBAoMEnN0YXRlLWluc3RpdHV0
aW9uczEUMBIGA1UEAwwLVGF4
IENBIFRlc3QwHhcNMTUwNzIzMTUyOTA1WhcNMzUw
NzIzMTUyOTA1WjBAMQswCQYD
VQQGEwJTSTEbMBkGA1UECgwSc3RhdGUtaW5zdGl
0dXRpb25zMRQwEgYDVQQDDAtU
YXggQ0EgVGVzdDCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBALmH3XNA
KDgN8+G2jX4W/a7LTER10VbRhkGeuc9zyOuj9gigYXL
no4Im/S4iXMcCs1IxgSsj
NJ1YMOje4qgHbFKQwWV588VDw7/fiMMZIXvFjHfladd
HASEDMT53bKX3HIdJZ/iL
6xhpJ/+C/I8dnWcMZUkeP+9BUAni/I2xrHaAVIli0aS6uc/
DjO7b4Gj1Vl4FGIHo
DIH+LmWz26P2gg2xnpWgIxXzs5sN8nYErwu+6h/9xRE
Hco8PPCAZb5HZhqoIzYzk
N1S1Do6qAzt/wJM0mhWOWHt9fhp/RoYQ5ZFClZmgd1
cJcr6S6U7ebAQ+yYRsIWU5
+FLYZ4Zlt3ZAHNWyraMee/kFsaGcO21cwE+tPDOIn41
B8XvfaXApQt4+TejZWzoH
V0ojA+9H8V+wCFVMJssViFOzuS6SlEZ/xzslo+B//cfUkq
/PnWLJHEy4BJXsj4+F
CvliZ7Lq3B/RcQmBjmTRQ0mxahiMGrrQW4TLjUYgY8If
wKfMfwFwVwUyk5br9Grs
UX7jy7+Xx17Qed4p0jjOC7KutzRIGr6ULSk11qpd5IHeI
wzSOaTXk6rAzZYupPH5
```

```
KvY65mdRfq0C0cB2bMvk9m9lyeLfZz5+L9XDLlodTdw
OeWaKvjFErT8WSEkpHxtG
q13TVgicoxsHC2K+8hpFjpaz69ZCmTzj4/17AgMBAAGj
QjBAMB0GA1UdDgQWBBQz
zVr7CUfHAeY2KCb1gXy3jjX3sjAPBgNVHRMBAf8EBTA
DAQH/MA4GA1UdDwEB/wQE
AwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAR9xtbaNa/jS
AAyqe3aq88GG7rCyxROGH
BPcakfMmhx1cLYdcY5ATXL/n67eo+S+1g7e/sK3fVXav
5qWs9oUEhAOgcOACMohu
JlBbMq2Qp8lxdpiRWCcyiY1vGQcHcZ02oey/c06fBZE4i
qJdYAhYhsBB5H+idtwJ
s6Lade4wqG58hWCNKBxU+KWDckGGX5CxsfU7gdYgj
yKq0ow60qQWi4H8pD+WO1Bn
rvISkAT7vMk2BOz+YlCKZmuq0h3PCkK5T6xA01fUZCa
eze0RozFaekDBEHK0bc1D
My3SKbB3cjdcMzmV8sVdxnNOTxlrP7+BinctxT3q3Va9
6kTmwI5pD0x6KOwC7Urr
53ubhI3U2XBAzkk14lDLU+7tqBqhDWwIMN0NyW1MR
TF8JB9Rz+4yCcDWMOT/FZg7
C60RrcnaO/0GETDz6XI6zedBXo1Q/rJTtXMOr8iVnc+jo
ZyO2ImOuTwP3C7M3Bnp
gFHqDtD48n9PV9prhbD4fYPyMe/3rshtBcpGAy2cGjpsP
28pkvP8lwBaP8pnpxvQ
7d3oiCBzznaOHjhm8+8C53b/1txzj/LP/4ZzlynsOhxy4cih
EPhAg1MKUY9qnbw9
9Q6EKrCSqk3TPqiWrTtu4pxyiEiquCHk8n+HX5cVhxUk
aEShdx4bjgvKB7JRF2T2
ST1lrKEM2DY=
-----END CERTIFICATE-----
OK
AT+CCERTLIST                                    // list certificate files
+CCERTLIST: "&#x4E2D;&#x534E;.pem"
+CCERTLIST: "client_key.der"

OK
```