SSL Application Note

Document Title:	SIM 5360 SSL Application Note
Version:	0.01
Date:	2014-02-24
Status:	Developing
Document ID:	SIM5360_SSL_Application_Note_V0.01

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 Limited., copying of this document and giving it to others and the using or communication of the contents thereof, are forbidden without express authority. Offenders are liable to the payment of damages. All rights reserved in the event of grant of a patent or the registration of a utility model or design. All specification supplied herein are subject to change without notice at any time.

Copyright © Shanghai SIMCom Wireless Solutions Ltd. 2013

Version History

Version	Chapter	Comments
V0.01	New Version	

Contents

1. Introduction

1.1 Overview

This document gives the usage of SIM52XX SSL functions; user can get useful information about the SIM52XX SSL functions quickly through this document.

The SSL functions are provided in AT command format, and they are designed for customers to design their HTTPS,FTPS and common SSL applications easily. User can access the SSL AT commands through UART/ USB interface which communicates with SIM52XX module.

SIM52XX SSL features:

- Basic HTTPS GET and POST operations.
- Basic FTPS LOGIN, LOGOUT, LIST, DEL, RMD, MKD, GET, PUT operations.
- Basic SSL socket operations.

1.2 References

The present document is based on the following documents:

SIMCOM_SIM5360_ATC_EN_V0.05.doc

1.3 Terms and Abbreviations

For the purposes of the present document, the following abbreviations apply:

- AT ATtention; the two-character abbreviation is used to start a command line to be sent from TE/DTE to TA/DCE
- EDGE Enhanced Data GSM Environment
- EGPRS Enhanced General Packet Radio Service
- FTPS File Transfer Protocol over Secure socket Layer
- GPRS General Packet Radio Service
- GSM Global System for Mobile communications
- HTTPS Hypertext Transfer Protocol over Secure Socket Layer
- PIN Personal Identification Number
- SSL Secure Socket Layer
- TA Terminal Adaptor; e.g. a data card (equal to DCE)
- TE Terminal Equipment; e.g. a computer (equal to DTE)
- UMTS Universal Mobile Telecommunications System
- URC Unsolicited Result Code
- USIM Universal Subscriber Identity Module

- WCDMA Wideband Code Division Multiple Access

2. HTTPS operations

The purpose of this section is to help get you start with HTTPS operations.

2.1 Acquire HTTPS stack

Each time when user needs to access a new HTTPS URL (AT+CHTTPSOPSE), the HTTPS stack needs to be acquired before the HTTPS operations:

AT+CHTTPSSTART
OK

2.2 Connect HTTPS server

After acquiring the HTTPS stack, user can connect the HTTPS server using the following AT command:

AT+CHTTPSOPSE="www.mywebsite.com", 443, 2
OK

The last parameter is the server type. Default is 2(HTTPS server). Following are the HTTPS server that supported:

1-HTTP server
2-HTTPS server with SSL3.0/TLS1.0 supported

2.3 Send HTTPS Request

After the HTTPS connection is established successfully. User can send HTTPS request data using the following AT commands:

AT+CHTTPSSEND=88
>GET / HTTP/1.1
Host: www.mywebsite.com
User-Agent: MY WEB AGENT
Content-Length: 0

OK

When the HTTPS data is large (for example, posting a large file to server), the AT+CHTTPSSEND can be used to send the data segmented to multiple parts:

AT+CHTTPSSEND=1024
…
AT+CHTTPSSEND=1024
…

When all the data has been sent, the AT+CHTTPSSEND is used to commit these request data:

AT+CHTTPSSEND
OK
…
+CHTTPSSEND: 0

Also user can query how much data in the module cache is waiting to be sent:

AT+CHTTPSSEND?
+CHTTPSSEND: 1024
OK

2.4 Receive HTTPS response

After sending the HTTPS data, the HTTPS server may send HTTPS response to the module, and the module can use the following command to receive data from the server:

AT+CHTTPSRECV=1
OK
+HTTPSRECV: DATA,249
HTTP/1.1 200 OK
Content-Type: text/html
Content-Language: zh-CN
Content-Length: 57
Date: Tue, 31 Mar 2009 01:56:05 GMT
Connection: Close
Proxy-Connection: Close

<html>
<header>test</header>
<body>
Test body
</body>

+CHTTPSRECV: 0

The parameter of this command is used to tell the module to receive the response data with at

least the length of the parameter.

If the response data is very large, user can use AT+CHTTPSRECV to receive the data multiple times.

2.5 Close HTTPS connection

User can close the HTTPS connection using AT+CHTTPSCLSE

AT+CHTTPSCLSE
OK

2.6 Release HTTPS stack

After closing HTTPS connection, user must release the HTTPS stack:

AT+CHTTPSSTOP
OK

2.7 Timer values of HTTPS operation

Following are the timer value setting for HTTPS operation:

Timer	Value
HTTPS connect	2 minutes
HTTPS transferring timer	2 minutes
HTTPS close	2 minutes
HTTPS stop wireless network	2minutes

3. FTPS operations

3.1 Acquire FTPS stack

Each time when user needs to access a FTPS server, the FTPS stack needs to be acquired first:

AT+CFTPSSTART
OK
+CFTPSSTART: 0

3.2 Login the FTPS server

User can use the following AT command to login the FTPS server:

AT+CFTPSLOGIN="www.myftpsserver.com", 990, "myname", "mypassword",3
OK
+CFTPSLOGIN: 0

The last parameter of AT+CFTPSLOGIN is the type of FTP/FTPS server. Default is 3(implicit FTPS server). Following are the supported FTP/FTPS server type:
0-FTP server
1-explicit FTPS server with AUTH SSL supported
2-explicit FTPS server with AUTH TLS supported
3-implicit FTPS server with SSL3.0/TLS1.0 supported

3.3 Get Current directory on FTPS server

The following command can be used to get the current FTPS directory on server:

AT+CFTPSPWD
+CFTPSPWD: "/"
OK

3.4 Change Current directory on FTPS server

The following command can be used to change the current FTPS directory on server:

AT+CFTPSCWD= "/mysubdir"
OK

3.5 Create a new directory on FTPS server

The following command can be used to create a new directory on FTPS server:

AT+CFTPSMKD= "mynewdir"
OK

3.6 Remove a directory on FTPS server

The following command can be used to remove a directory on FTPS server:

AT+CFTPSRMD= "mynewdir"
OK

Only when directory is empty, the directory can be removed successfully.

3.7 Delete a file on FTPS server

The following command can be used to delete a file on FTPS server:

AT+CFTPSDEL= "mydelfile"
OK

3.8 Set FTPS transfer type

The following command can be used to set FTPS transfer type:

AT+CFTPSTYPE= I
OK

3.9 List all items in current directory on FTPS server

The following command can be used to list all items in current directory on FTPS server:

AT+CFTPSLIST
OK
+CFTPSLIST: DATA,193
drw-rw-rw- 1 user group 0 Sep 1 18:01 .
drw-rw-rw- 1 user group 0 Sep 1 18:01 ..
-rw-rw-rw- 1 user group 2017 Sep 1 17:24 19800106_000128.jpg

+CFTPSLIST: 0

3.10 Put a file from EFS to FTPS server

The following command can be used to put a file from EFS to FTPS server:

AT+CFTPSPUTFILE= 1, "myputlfile.txt"
OK
+CFTPSPUTFILE: 0

3.11 Put a file from external MCU to FTPS server

The following command can be used to put a file from external MCU to FTPS server:

AT+CFTPSPUT= "myputlfile.txt", 10
>test content
OK

When the file is large, user can use the following commands after the previous command to put the left data:

AT+CFTPSPUT=1024
>…
OK
AT+CFTPSPUT=1024
>…
OK

After user has put all the data, the AT+CFTPSPUT should be used to put all the data:

AT+CFTPSPUT
OK
+CFTPSPUT: 0

Also user can use AT+CFTPSPUT? to query the size of the data in the module cache which needs to be sent:

AT+CFTPSPUT?
+CFTPSPUT: 1024
OK

3.12 Get a file from FTPS server to EFS

The following command can be used to get a file from FTPS server to EFS:

AT+CFTPSGETFILE= 1, "mygetlfile.txt"
OK

+CFTPSGETFILE: 0

3.13 Get a file from FTPS server to external MCU

The following command can be used to get a file from FTPS server to external MCU:

AT+CFTPSGET= "myputlfile.txt"
OK
+CFTPSGET: DATA, 1020,
…
+CFTPSGET: DATA, 1058,
…
…
+CFTPSGET: 0

3.14 Logout the FTPS server

User can use the following AT command to logout the FTPS server:

AT+CFTPSLOGOUT
OK
+CFTPSLOGOUT: 0

3.15 Release the FTPS stack

User can use the following AT command to release FTPS stack:

AT+CFTPSSTOP
OK
+CFTPSSTOP: 0

3.16 Timer values of FTPS operation

Following are the timer value setting for FTPS operation:

Timer	Value
HTTPS connect	2 minutes
HTTPS transferring timer	2 minutes
HTTPS close	2 minutes
HTTPS stop wireless network	2minutes

4. Common Channel operations

The purpose of this section is to help get you start with common SSL operations.

4.1 Set sending URC and receive data mode

Ths following command can be used to set sending result URC and receive data mode:

AT+CCHSET=0, 0
OK

The first parameter is the AT+CCHSEND URC report mode. If it is set to 1, after sending complete, the +CCHSEND: <session>,<result_code> will be reported.

The second parameter is the AT+CCHRECV mode. When it is 0, each received data packet will be reported as URC like +CCHRECV: DATA,<session_id>,<len>\r\n<data> directly. If the parameter is set to 1, whenever there is new data packet arrived, the +CCHEVENT: <session_id>,RECV EVENT URC will be reported, then MCU can use AT+CCHRECV=<session_id> to retrieve the received data.

4.2 Acquire Common Channel stack

The common channel stack needs to be acquired using the following AT command:

AT+CCHSTART
OK
+CCHSTART: 0

4.3 Open the channel

After acquiring the common channel stack, user can connect to peer using the following AT command:

*AT+CCHOPEN=**1**, "www.mydomain.com" , 443,2*
OK
+CCHOPEN: 1, 0

The first parameter in all common channel related commands and unsolicited result code is the channel id. Currently only 0 and 1 are valid, which means there are maximum two sessions can be established at the same time.

The fourth parameter is the channel type, following are the supported channel types:

0-UDP
1-TCP client
2-SSL client with SSL3.0/TLS1.0 supported(default)

4.4 Send data

After the channel is opened successfully. User can send data using the following AT commands:

*AT+CCCHSEND=**1**, 88*
>…0

OK

When the data is large, the AT+CCHSEND can be used to send for multiple times:

*AT+CCHSEND=**1**, 1024*
>…
*AT+CCHSEND=**1**, 1024*
>…

When AT+CCHSET=1 is set, the +CCHSEND URC will be report after sending:

*+CCHSEND: **1**, 0*

Also user can query how much data in the module cache is waiting to be sent:

AT+CCHSEND?
*+CCHSEND: **0**, 0, **1**, 1024*
OK

4.5 Receive data

When the second parameter of AT+CCHSET is 0, whenever there is data arrived, the following unsolicited code may be reported:

*+CCHRECV: DATA, **1**, 1024*
.....
When the second parameter of AT+CCHSET is 1, whenever there is data arrived, the following unsolicited code may be reported:
+CCHEVENT: 1, RECV EVENT
The MCU can use AT+CCHRECV=1 to retrieve the cached received data

4.6 Close the channel

User can close the SSL connection using AT+CSSLCLOSE

*AT+CCHCLOSE = **1***
OK
*+CCHCLOSE: **1**, 0*

4.7 Release the stack

After closing all the opened channels, user must release the common channel stack:

AT+CCHSTOP
OK
+CCHSTOP: 0

4.8 Using Transparent Mode for Common Channel Service

Currently only session 0 can be used for transparent mode. If user needs to use transparent mode for common channel AT commands, the following AT command needs to be executed:

AT+CCHMODE=1
OK

After running this command, the AT+CCHOPEN command will run like following:

AT+CCHMODE=1
OK
AT+CCHSTART
OK
AT+CCHOPEN=0,"www.myserver.com",443
CONNECT 115200
…..

When the "CONNECT 115200" is reported, the current serial port is running in SSL transparent mode, all the data put into the port will be transferred to the peer part transparently, and all the data received from the peer part will be output through the serial port. If the UART or USB MODEM port is used to run this command, the "+++", DTR signal and ATO command can be used to switch the serial port mode between "ONLINE DATA" AND "ONLINE COMMAND".

4.9 Timer values of Channel operation

Following are the timer value setting for SSL operation:

Timer	Value
Open channel	2 minutes
Waiting sendable state	2 minutes
Channel close	2 minutes
Release common channel stack	2minutes

5. Unsolicited Result Code

5.1 Unsolicited result code of HTTPS

Code	Description
+CHTTPS: RECV EVENT	When the AT+CHTTPSRECV is not being called, and there is data cached in the receiving buffer, this event will be reported.

5.2 Unsolicited result code of common channel

Following is the unsolicited result code of +CCHRECV URC,

Code of <level>	Description
+CCHRECV: DATA, <session_id>,<len>\r\n<data>	The session_id is the index of the channel. The len is the length of the data.

6. Certificate & Key Management

The purpose of this section is to help get you start with common SSL certificate & key management. Currently only .der and raw .pem format files without password protection can be used.

6.1 Download certificate & key files to the module

Ths following command can be used to download certificate & key files to the module:

AT+CCERTDOWN=”mycert.der”, 753
>file content...
OK

Following is the sample source code for calling AT+CCERTDOWN:


certdownloader_src.rar

6.2 List all certificate & key files in the module

The following command can be used to list all the certificate & key files which has been downloaded into the module:

AT+CCERTLIST
+CCERTLIST: "ca_cert.der"
+CCERTLIST: "client_cert.der"
+CCERTLIST: "client_key.der"
+CCERTLIST: "server_cert.pem"
+CCERTLIST: "server_key.pem"

OK

6.3 Delete a certificate or key file in the module

The following command can be delete a certificate & key file which has been downloaded into the module:

AT+CCERTDELE=” server_key.pem”
OK

6.4 Set the CA file

The following command can be used to set the CA file for current SSL operation, This command can only be used after AT+CHTTPSSTART/AT+CCHSTART/AT+CFTPSSTART:

AT+CCERTCA=0,"ca.pem"
OK

6.5 Set the certificate file

The following command can be used to set the certificate file for current SSL operation, This command can only be used after AT+CHTTPSSTART/AT+CCHSTART/AT+CFTPSSTART:

AT+CCERTCERT="my_cert.pem",0
OK

6.6 Set the key file

The following command can be used to set the key file for current SSL operation, This command can only be used after AT+CHTTPSSTART/AT+CCHSTART/AT+CFTPSSTART:

AT+CCERTKEY=0,"my_key.pem"
OK

6.7 Load the CA/certificate/key files

The following command can be used to load the CA/certificate/key files set using AT+CSSLCA/AT+CSSLCERT/AT+CSSLKEY for current SSL operation, This command can only be used after AT+CHTTPSSTART/AT+CCHSTART/AT+CFTPSSTART:

AT+CSSLLOADCK
OK

7. AT Command Samples

7.1 AT Command Samples of HTTPS

AT commands	Comments
AT+CHTTPSSTART OK	Acquire the HTTPS stack
AT+CHTTPSOPSE="www.mywebsite.com",443 OK	Connect the HTTPS server
AT+CHTTPSSEND=88 >GET / HTTP/1.1	Send the HTTPS request data. If the request is large, this AT+CHTTPSSEND=<len>

Host: www.mywebsite.com User-Agent: MY WEB AGENT Content-Length: 0 OK	command can be used multiple times.
AT+CHTTPSSEND	Commit all the data which has been sent previously using AT+CHTTPSSEND=<len>
AT+CHTTPSRECV=1 OK +CHTTPSRECV: DATA,249 HTTP/1.1 200 OK Content-Type: text/html Content-Language: zh-CN Content-Length: 57 Date: Tue, 31 Mar 2009 01:56:05 GMT Connection: Close Proxy-Connection: Close <html> <header>test</header> <body> Test body </body> +CHTTPSRECV: 0	Receive the HTTPS response from the HTTPS server. If the response data is large, this AT+CHTTPSRECV=<len> command can be used multiple times.
AT+CHTTPSCLSE OK	Close the HTTPS connection
AT+CHTTPSSTOP OK	Release the HTTPS stack

7.2 AT Command Samples of FTPS

AT commands	Comments
AT+CFTPSSTART OK +CFTPSTART: 0	Acquire the FTPS stack
AT+CFTPSLOGIN=*"www.myftpsserver.com",990, "myname", "mypassword"* OK +CFTPSLOGIN: 0	Login the FTPS server
AT+CFTPSMKD="testdir"	Create a directory under the current directory

OK	on FTPS
AT+CFTPSRMD=”testdir”	Remove a directory from the current directory on FTPS server
AT+CFTPSDEL=”testdelfile.txt” OK	Delete a file on the FTPS server
AT+CFTPSCWD=”/mysubdir” OK	Change current directory to “/mysubdir” on FTPS server
AT+CFTPSPWD +CFTPSPWD:”/mysubdir” OK	Get the current directory on FTPS server
AT+CFTPSTYPE=I	Set the FTPS transferring type to binary
AT+CFTPSLIST +CFTPSLIST: DATA,193 drw-rw-rw- 1 user group 0 Sep 1 18:01 . drw-rw-rw- 1 user group 0 Sep 1 18:01 .. -rw-rw-rw- 1 user group 2017 Sep 1 17:24 19800106_000128.jpg +CFTPSLIST: 0	List the items under the current directory on FTPS server
AT+CFTPSGETFILE=1, ”testfile.jpg” OK +CFTPSGETFILE: 0	Get the “testfile.jpg” from server to local EFS C:\Picture directory
AT+CFTPSPUTFILE=1, ”testfile.jpg” OK +CFTPSPUTFILE: 0	Put the local C:\Picture\testfile.jpg to the current directory on FTPS server
AT+CFTPSGET=”testfile.jpg” OK +CFTPSGET: DATA, 1024, … +CFTPSGET:DATA, 1058 … +CFTPSGET: 0	Get the “testfile.jpg” under current FTPS directory to external MCU.
AT+CFTPSPUT=”t1.txt”,11 >test content OK AT+CFTPSPUT=18 >left data put here OK AT+CFTPSPUT OK +CFTPSPUT: 0	Put a file of “t1.txt” from external MCU to the current directory on FTPS server.

AT+CFTPSLOGOUT OK +CFTPSLOGOUT: 0	Logout the FTPS server
AT+CFTPSSTOP OK +CFTPSSTOP: 0	Release the FTPS stack

7.3 AT Command Samples of Common Channel

AT commands	Comments
AT+CCHSET=1 OK	Enable reporting +CHSEND result
AT+CCHSTART OK +CCHSTART: 0	Accquire the common channel stack
AT+CCHOPEN=1, ”www.myserver.com”,443 OK	Connect the server
AT+CCHSEND=1, 88 >GET / HTTP/1.1 Host: www.mywebsite.com User-Agent: MY WEB AGENT Content-Length: 0 OK +CCHSEND: 1, 0	Send the data. If the request is large, this AT+CCHSEND=1, <len> command can be used multiple times.
+CCHRECV: DATA, 1, 249 HTTP/1.1 200 OK Content-Type: text/html Content-Language: zh-CN Content-Length: 57 Date: Tue, 31 Mar 2009 01:56:05 GMT Connection: Close Proxy-Connection: Close <html> <header>test</header> <body> Test body </body>	Receive the data sent from the peer.
AT+CCCHCLOSE=1 OK	Close the channel

AT+CCHLSTOP OK	Release the stack

7.4 AT Command Samples of HTTPS supporting cert/key

AT commands	Comments
AT+CHTTPSSTART OK	Acquire the HTTPS stack
AT+CSSLCA=0,"ca_cert.der" OK	Set the CA
AT+CSSLCERT="client_cert.der",0 OK	Set the client certificate
AT+CSSLKEY="client_key.der" OK	Set the client key
AT+CSSLLOADCK OK	Load the CA/certificate/key files
AT+CHTTPSOPSE=”www.mywebsite.com”,443 OK	Connect the HTTPS server
AT+CHTTPSSEND=88 >GET / HTTP/1.1 Host: www.mywebsite.com User-Agent: MY WEB AGENT Content-Length: 0 OK	Send the HTTPS request data. If the request is large, this AT+CHTTPSSEND=<len> command can be used multiple times.
AT+CHTTPSSEND	Commit all the data which has been sent previously using AT+CHTTPSSEND=<len>
AT+CHTTPSRECV=1 OK +CHTTPSRECV: DATA,249 HTTP/1.1 200 OK Content-Type: text/html Content-Language: zh-CN Content-Length: 57 Date: Tue, 31 Mar 2009 01:56:05 GMT Connection: Close Proxy-Connection: Close <html>	Receive the HTTPS response from the HTTPS server. If the response data is large, this AT+CHTTPSRECV=<len> command can be used multiple times.

<header>test</header> <body> Test body </body> +CHTTPSRECV: 0	
AT+CHTTPSCLSE OK	Close the HTTPS connection
AT+CHTTPSSTOP OK	Release the HTTPS stack

7.5 AT Command Samples of Common Channel supporting cert/key

AT commands	Comments
AT+CCHSET=1 OK	Enable reporting +CHSEND result
AT+CCHSTART OK +CCHSTART: 0	Accquire the common channel stack
AT+CSSLCA=0,"ca_cert.der" OK	Set the CA
AT+CSSLCERT="client_cert.der",0 OK	Set the client certificate
AT+CSSLKEY="client_key.der" OK	Set the client key
AT+CSSLLOADCK OK	Load the CA/certificate/key files
AT+CCHOPEN=1, ”www.myserver.com”,443 OK	Connect the server
AT+CCHSEND=1, 88 >GET / HTTP/1.1 Host: www.mywebsite.com User-Agent: MY WEB AGENT Content-Length: 0 OK	Send the data. If the request is large, this AT+CCHSEND=1, <len> command can be used multiple times.

+CCHSEND: 1, 0	
+CCHRECV: DATA, 1, 249 HTTP/1.1 200 OK Content-Type: text/html Content-Language: zh-CN Content-Length: 57 Date: Tue, 31 Mar 2009 01:56:05 GMT Connection: Close Proxy-Connection: Close <html> <header>test</header> <body> Test body </body>	Receive the data sent from the peer.
AT+CCCHCLOSE=1 OK	Close the channel
AT+CCHLSTOP OK	Release the stack

8. Conflict AT Commands

The HTTPS, FTPS, Common SSL AT commands cannot run together and they also cannot be used when other socket related function is running:

- TCP/IP Related AT Commands.
- MMS AT Commands
- GPS AT Commands
- HTTP AT command
- FTP AT command

Contact us

Shanghai SIMCom Wireless Solutions Ltd.

Add: Building A, SIM Technology Building, No.633, Jinzhong Road, Changning District

200335

Tel: +86 21 3252 3300

Fax: +86 21 3252 3301

URL: http:/www.sim.com/wm/

Contact us

Shanghai SIMCom Wireless Solutions Ltd.
Add: Building A, SIM Technology Building, No.633, Jinzhong Road, Changning District
200335
Tel: +86 21 3252 3300
Fax: +86 21 3252 3301
URL: http:/www.sim.com/wm/