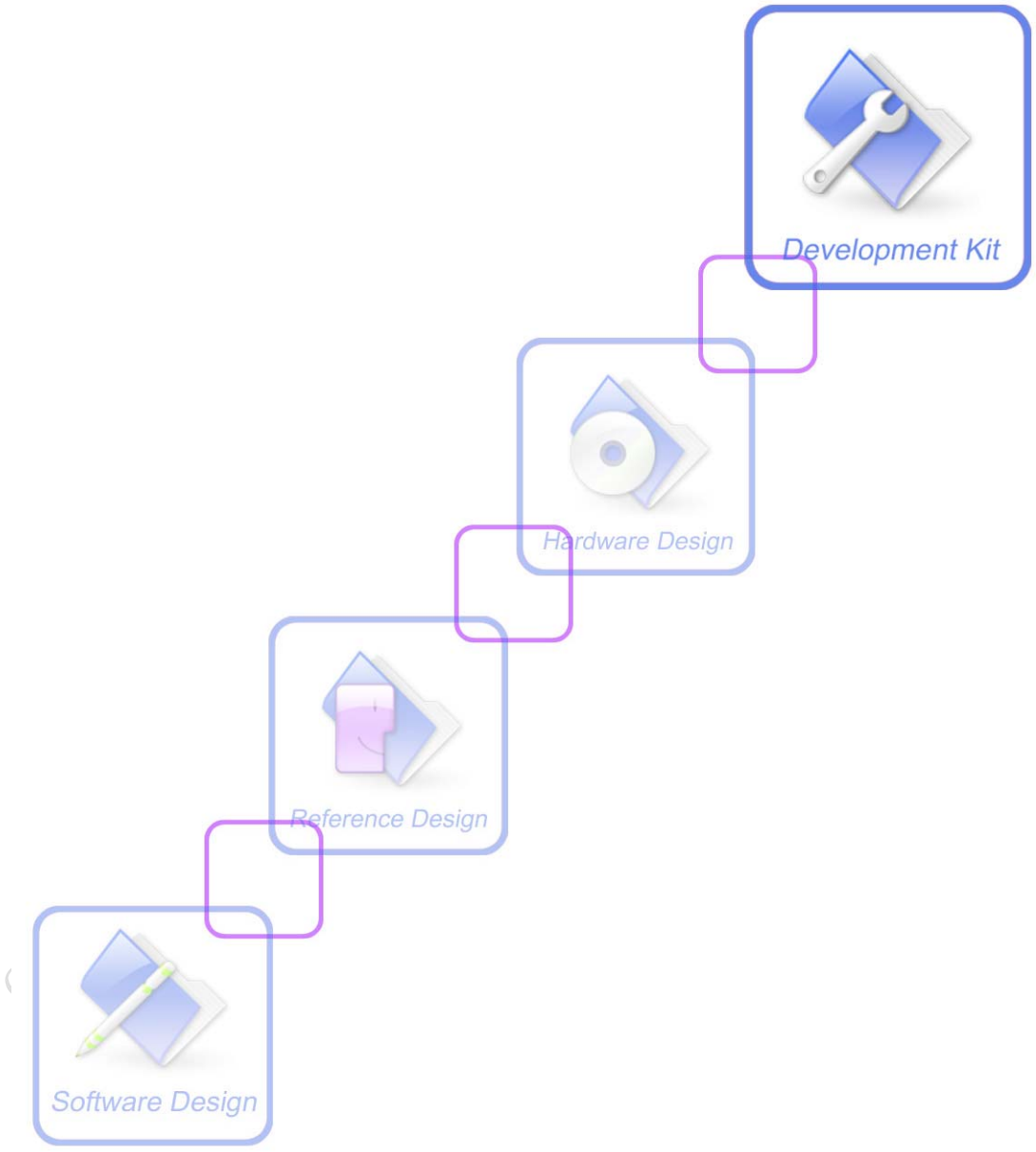
SSL **Application Note**



Document Title:	SIM52xx SSL Application Note
Version:	0.01
Date:	2012-08-22
Status:	Release
Document Control ID:	SIM52xx_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. 2010

SIMCOM Confidential, NDA Required

Version History

Version	Chapter	Comments
V0.01	New Version	

SIMCOM Confidential, NDA Required

Contents

Version History 2
Contents 3
1. Introduction....1
1.1 Overview....1
1.2 References....1
1.3 Terms and Abbreviations....1
2. HTTPS operations....1
2.1 Acquire HTTPS stack....1
2.2 Connect HTTPS server....1
2.3 Send HTTPS Request....1
2.4 Receive HTTPS response....2
2.5 Close HTTPS connection....3
2.6 Release HTTPS stack....3
2.7 Timer values of HTTPS operation....3
3. FTPS operations....3
3.1 Acquire FTPS stack....3
3.2 Login the FTPS server....3
3.3 Get Current directory on FTPS server....4
3.4 Change Current directory on FTPS server....4
3.5 Create a new directory on FTPS server....4
3.6 Remove a directory on FTPS server....4
3.7 Delete a file on FTPS server....4
3.8 Set FTPS transfer type....5
3.9 List all items in current directory on FTPS server....5
3.10 Put a file from EFS to FTPS server....5
3.11 Put a file from external MCU to FTPS server....5
3.12 Get a file from FTPS server to EFS....6
3.13 Get a file from FTPS server to external MCU....6
3.14 Logout the FTPS server....7
3.15 Release the FTPS stack....7
3.16 Timer values of FTPS operation....7
4. Common SSL operations....7
4.1 Acquire SSL stack....7
4.2 Connect the SSL server....8
4.3 Send SSL data....8
4.4 Receive SSL data....9
4.5 Close SSL connection....9
4.6 Release SSL stack....9
4.7 Using Transparent Mode for Common SSL....9
4.8 Timer values of SSL operation....10
5. Unsolicited Result Code....10
5.1 Unsolicited result code of HTTPS....10

SIMCom Confidential, NDA Required

5.2 Unsolicited result code of SSL 11
6. AT Command Samples 12
6.1 AT Command Samples of HTTPS 12
6.2 AT Command Samples of FTPS 13
6.3 AT Command Samples of Common SSL 14
7. Conflict AT Commands 15

SIMCOM Confidential, NDA Required

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:

[1] SIMCOM_WCDMA_Internet_Service_ATC_V1.04.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

SIMCOM Confidential, NDA Required

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
OK

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
…

SIMCOM Confidential, NDA Required

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.

SIMCOM Confidential, NDA Required

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

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”
OK

SIMCOM Confidential NDA Required

Currently only explicit FTPS mode is 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"

SIMCOM Confidential, NDA Required

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:

SIMCOM Confidential, NDA Required

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

SIMCOM Confidential NDA Required

3.14 Logout the FTPS server

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

AT+CFTPSLOGOUT
OK

3.15 Release the FTPS stack

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

AT+CFTPSSTOP
OK

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 SSL operations

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

4.1 Acquire SSL stack

Each time when user needs to access a new SSL server (AT+CSSLOPEN), the SSL stack needs to be acquired using the following SSL operations:

AT+CSSLSTART
OK

SIMCOM Confidential NDA Required

4.2 Connect the SSL server

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

AT+CSSLOPEN=1, "www.mydomain.com", 443
OK

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

When there is any alert occurred in SSL authentication, the following unsolicited code may be reported:

+CSSLALERT: 1, 0, 0

If user wants to continue the SSL opening session, the following command needs to be executed:

AT+CSSLCONT = 1
OK

If user wants to cancel the SSL opening session, the following command needs to be executed:

AT+CSSLCLOSE = 1
OK

4.3 Send SSL data

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

AT+CSSLSEND=1, 88
>…0

OK

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

AT+CSSLSEND=1, 1024

SIMCOM Confidential, NDA Required

>…
AT+CSSLSEND=1, 1024
>…

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

+CSSLSEND: 1, 0, 1024

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

AT+CSSLSEND?
+CSSLSEND: 0, 0, 1, 1024
OK

4.4 Receive SSL data

When there is data arrived, the following unsolicited code may be reported:

+CSSLRECV: DATA, 1, 1024
.....

4.5 Close SSL connection

User can close the SSL connection using AT+CSSLCLOSE

AT+CSSLCLOSE = 1
OK

4.6 Release SSL stack

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

AT+CSSLSTOP
OK

After running this command, both SSL connections will be closed.

4.7 Using Transparent Mode for Common SSL

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

SIMCOM Confidential, NDA Required

AT+CSSLMODE=1
OK

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

AT+CSSLMODE=1
OK
AT+CSSLSTART
OK
AT+CSSLOPEN=0,"www.myserver.com",443
+CSSLALERT: 0,2,134218240
+CSSLOPEN: ALERTSTATE
ERROR
AT+CSSLCONT=0
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".

4.8 Timer values of SSL operation

Following are the timer value setting for SSL operation:

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

SIM Confident Under NDA Required

	the receiving buffer, this event will be reported.

5.2 Unsolicited result code of SSL

Following is the unsolicited result code of +CSSLALERT: <session_id>, <level>, <err>

Code of <level>	Description
0	Warning
1	Fatal
2	Suspend
3	Information

The <err> code of +CSSLALERT is a multiple bits combination of error. Each bit has the following meaning:

Bit position of <err>	Description
0x00000001	SSL protocol received unexpected message
0x00000002	SSL record failed authentication
0x00000004	Decrypted message not multiple of block size, or invalid padding
0x00000008	Record too big
0x00000010	SSL record failed decompression
0x00000020	SSL handshake protocol failed
0x00000040	Certificate is missing
0x00000080	Certificate failed authentication
0x00000100	Certificate failed authentication of bad signature
0x00000200	Certificate failed authentication of bad issuer
0x00000400	Certificate type not understood
0x00000800	Certificate invalid (was revoked)
0x00001000	Certificate invalid (expired)
0x00002000	Certificate invalid (some error)
0x00004000	SSL protocol parameters out of range
0x00008000	Alert contained invalid ID
0x00010000	Unknown CA
0x00020000	No access rights to continue negotiation
0x00040000	Failed value out of range
0x00080000	Crypto operation failed
0x00100000	Parameter not in compliance
0x00200000	Cannot support requested version
0x00400000	Server requires more secure cipher suites than the client support
0x00800000	Local error independent of the protocol
0x01000000	Cancel handshake for other reasons
0x02000000	Cannot negotiate the handshake
0x04000000	Host mismatch (Common Name)

0x08000000	Alert to viewing the certificate
0x10000000	Alert for unrecognized server name list

Following is the unsolicited result code of +CSSL: RECV EVENT, <ssl_id>

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

6. AT Command Samples

6.1 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 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	Receive the HTTPS response from the HTTPS server. If the response data is large, this AT+CHTTPSRECV=<len> command can be used multiple times.

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

6.2 AT Command Samples of FTPS

AT commands	Comments
AT+CFTPSSTART OK	Acquire the FTPS stack
AT+CFTPLOGIN=*"www.myftpsserver.com",990, "myname", "mypassword"* OK	Login the FTPS server
AT+CFTPSMKD="testdir" OK	Create a directory under the current directory 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	List the items under the current directory on FTPS server

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

6.3 AT Command Samples of Common SSL

AT commands	Comments
AT+CSSLSET=1 OK	Enable reporting +CSSLSEND result
AT+CSSLSTART OK	Accquire SSL stack
AT+CSSLOPEN=1, ”www.myserver.com”,443 +CSSLALERT: 0,2,134218240 +CSSLOPEN: ALERTSTATE	Connect the SSL server

ERROR	
AT+CSSLCONT=1 OK	Continue to connect the SSL server.
AT+CSSLSEND=1, 88 >GET / HTTP/1.1 Host: www.mywebsite.com User-Agent: MY WEB AGENT Content-Length: 0 OK +CSSLSEND: 1, 0, 88	Send the SSL data. If the request is large, this AT+CSSLSEND=1, <len> command can be used multiple times.
+CSSLRECV: 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+CSSLCLOSE=1 OK	Close the SSL connection
AT+CSSLSTOP OK	Release the SSL stack

7. 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/

SIMCOM Confidential, NDA Required

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/

SIMCOM Confidential, NDA Required