A company of SIM Tech

SIMCom_3G_SSL_Application Note_V1.10

Document Title:	SIMCom_3G_SSL_Application Note
Version:	1.10
Date:	2014-12-23
Status:	Release
Document Control ID:	SIMCom_3G_SSL_Application Note_V1.10

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

Contents

Version History

Date	Version	Description of change	Author
2013-18-01	V1.00	New version	songjin
2013-12-27	V1.10	Rewrite using new document template	songjin

Scope

This document presents the AT command of SSL operation and application examples. This document can apply to SIMCom 3G modules, including SIM5218/SIM5215/SIM5216/SIM5320/SIM5310/SIM6320/SIM6216 series modules.

1 Introduction

This document presents the AT command of SSL operation for SIMCom 3G modules.

1.1 Features

1. SIMCom 3G series supports SSL certificate and key management AT operation.
2. SIMCom 3G series supports transfer over SSL(common channel/HTTPS/FTPS/SMTPS).
3. SIMCom 3G series SSL supports SSL3.0/TLS1.0.

2 AT commands

Below is the email associated with AT commands, detailed information please refer to document [1].

Through these AT commands can achieve the following functions.

1) Open common channel session.
2) Close common channel session
3) Send data using common channel
4) Receive data using common channel

Command	Description
AT+CCHMODE	Set data mode or command mode
AT+CCHSET	Set send result URC and receive mode.
AT+CCHSTART	Start common channel stack, also active the PDP context
AT+CCHSTOP	Stop common channel stack, also deactive the PDP context
AT+CCHOPEN	Open common channel session
AT+CCHCLOSE	Close common channel session
AT+CCHSEND	Send data
AT+CCHRECV	Read data in cache buffer
AT+CCHSTATE	Get the state of common channel stack
AT+CCERTDOWN	Download certificate/key files to module
AT+CCERTLIST	List all certificate/key files in module
AT+CSSLCA	Set CA file
AT+CSSLCERT	Set certificate file
AT+CSSLKEY	Set key file
AT+CSSLLOADCK	Load the CA/certificate/key files

3 Examples

There are some examples to explain how to use these commands.

In the "Grammar" columns of following tables, input of AT commands are in black , module return values are in blue.

3.1 Bearer Profile

Grammar	Description
AT+CGSOCKCONT=1,”IP”,”apn” OK AT+CSOCKSETPN=1 OK	Configure bearer profile 1

3.2 Start Common Channel Stack

Common channel is a set of AT commands which provides common operation for UDP/TCP client/SSL like OPEN/CLOSE/SEND DATA/RECEIVE DATA.

Grammar	Description
AT+CCHSTART OK +CCHSTART: 0	Start common channel stack

3.3 Open Common Channel Session

Grammar	Description
AT+CCHOPEN=0,”www.myhttpserver.com”,443,2 OK +CCHOPEN: 0,0	Open common channel session<0>. The red parameter defined in the following: 0-UDP socket 1-TCP client socket 2- SSL client with SSL3.0/TLS1.0 supported(default)

3.4 Send Small Data

Grammar	Description

AT+CCHSEND=0,88 >GET / HTTP/1.1 Host: www.mywebsite.com User-Agent: MY WEB AGENT Content-Length: 0 OK	Send data
+CCHSEND: 0,0	If the AT+CCHSET=1 is set, and all data has been sent, the +CCHSEND URC will be report

3.5 Send Large Data

Grammar	Description
AT+CCHSEND=0,1024 >…(data of 1024 bytes) OK … AT+CCHSEND=0,1024 >…(data of 1024 bytes) OK	Send data to server
AT+CCHSEND? +CCHSEND: 0,**10812**,1,0 OK	Check how many data is left in sending buffer. If the cached data is more than 10K bytes, the program should wait some seconds an check the AT+CCHSEND? again to make sure there is free buffer in module to continue to call AT+CCHSEND=<session_id>,<len>.
+CCHSEND: 0,0	If the AT+CCHSET=1 is set, and all data has been sent, the +CCHSEND URC will be report
AT+CCHSEND? +CCHSEND: 0,**0**,1,0 OK	Now no data cached in sending buffer. Usually we can continue to send data when the data cached <= 3K bytes.
AT+CCHSEND=1024 >…(data of 1024 bytes) OK	Continue to send data.

… AT+CCHSEND=576 >…(data of 576 bytes) OK	
+CCHSEND: 0,0	If the AT+CCHSET=1 is set, and all data has been sent, the +CCHSEND URC will be report
AT+CCHSEND? +CCHSEND: 0,0,1,0 OK	Now no data cached in sending buffer. All data has been sent.

3.6 Receive Data Automatically

Grammar	Description
+CHTTPSRECV: DATA,0,1024 …(data of 1024 bytes) +CHTTPSRECV: 0 … +CHTTPSRECV: DATA,0,1024 …(data of 1024 bytes) +CHTTPSRECV: 0 +CHTTPSRECV: DATA,0,100 …(data of 100 bytes) +CHTTPSRECV: 0	The +CHTTPSRECV: DATA,<session_id>,<len> will be reported whenever there is data received in “automatic” mode.

3.7 Receive Data Manually

By default, the receive mode is “automatic” mode. The AT+CCHSET can be used to set the receive mode to “manual” mode. For example: AT+CCHSET=1,1. This command can only be called before AT+CCHSTART.

Grammar	Description
+CCHEVENT: 0,RECV EVENT	There is new data received in cache buffer.
AT+CCHRECV? +CCHRECV: LEN,4196,0 OK	Check how many data cached in receiving buffer.

AT+CCHRECV=0,1024 +CCHRECV: DATA,0,1024 …(data of 1024 bytes) +CCHRECV: 0 +CCHRECV: 0,RECV EVENT … AT+CCHRECV=0,1024 +CCHRECV: DATA,0,1024 …(data of 1024 bytes) +CCHRECV: 0 +CCHRECV: 0,RECV EVENT AT+CCHRECV=0,100 +CCHRECV: DATA,0,100 …(data of 100 bytes) +CCHRECV: 0	Read all data in cache buffer. Any time, the +CCHRECV: <session_id>,RECV EVENT indicates there is received data in cache buffer.

3.8 Close Common Channel Session

Grammar	Description
AT+CCHCLOSE=0 OK +CCHCLOSE: 0,0	Close common channel session<0>.

3.9 Stop Common Channel Stack

Grammar	Description
AT+CCHSTOP OK +CCHSTOP: 0	Stop common channel stack

3.10 Data Mode(Transparent mode)

Grammar	Description
AT+CCHMODE=1 OK	Set common channel module to use transparent mode. By default, it is 0(AT command mode).
AT+CCHSTART	Activate PDP context.

OK +CCHSTART: 0	
AT+CCHOPEN=0,"TCP","www.myhttpserver.com",443,2 CONNECT 115200	Connect to server. only session<0> is allowed to operate with transparent mode.
+++ OK	Sequence of +++ to quit data mode
AT+CCHCLOSE=0 OK CLOSED +CCHCLOSE: 0,0	Close session.
AT+CCHSTOP OK +CCHSTOP: 0	Deactivate PDP Context

3.11 Use SSL Certificates and Key Files

3.11.1 Download Certificate/Key Files to Module

Grammar	Description
AT+CCERTDOWN="mycert.der", 753 >file content of 753 bytes... OK	Download certificate/key files to module

3.11.2 List All Certificate/Key Files in the Module

Grammar	Description
AT+CCERTLIST +CCERTLIST: "ca_cert.der" +CCERTLIST: "client_cert.der" +CCERTLIST: "client_key.der" OK	List all certificate/key files in the module.

3.11.3 Delete Certificate/Key Files in the Module

Grammar	Description
AT+CCERTDELE="client_cert.der" OK	Delete certificate/key files.

3.11.4 Set 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:

Grammar	Description
AT+CCERTCA=0, "ca.pem" OK	Set CA File

3.11.5 Set 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:

Grammar	Description
AT+CCERTCERT="my_cert.pem",0 OK	Set Certificate File

3.11.6 Set 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:

Grammar	Description
AT+CCERTKEY=0,"my_key.pem" OK	Set Key File

3.11.7 Load 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:

Grammar	Description

AT+CSSLLOADCK OK	Set Certificate File

3.11.8 Use Certificate/Key Files for Common Channel

The AT+CSSLCA/AT+CSSLCERT/AT+CSSLKEY/AT+CSSLLOADCK must be put after +CCHSTART: 0 and before opening any common channel session.

Grammar	Description
AT+CCHSTART OK +CCHSTART: 0	Start 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=0,"www.myhttpserver.com", 443,2 OK +CCHOPEN: 0,0	Connect to SSL server.
AT+CCHCLOSE=0 OK +CCHCLOSE: 0,0	Close common channel session
AT+CCHSTOP OK +CCHSTOP: 0	Stop common channel stack

Appendix

A Related Documents

SN	Document name	Remark
[1]	SIMCOM_SIM5215_SIM5216_ATC_EN_V1.24.doc	

B Terms and Abbreviations

Abbreviation	Description
FTPS	FTP over SSL
HTTPS	HTTP over SSL
SSL	Secure Socket Layer

Contact us:
Shanghai SIMCom Wireless Solutions Co.,Ltd.
Address: Building A, SIM Technology Building, No. 633, Jinzhong Road, Shanghai, P. R. China 200335
Tel: +86 21 3252 3300
Fax: +86 21 3252 2030
URL: www.sim.com/wm