A company of SIM Tech

SIM800 Series_SSL_Application Note_V1.01

Document Title:	SIM800 Series_SSL_Application Note
Version:	1.01
Date:	2014-06-30
Status:	Release
Document Control ID:	SIM800 Series_SSL_ Application Note_V1.01

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

Contents

Version History

Date	Version	What is new	Author
2013-10-18	1.00	New version	Hanjun.Liu
2013-06-30	1.01	Chapter Scope, change projects	Jumping
		Chapter2.4, Add description of TCP over SSL	Hanjun.Liu
		Chapter2.5, Add description of import SSL certificate	Hanjun.Liu
		Chapter2.6, Add description of SSL option	Jumping
		Chapter3.8, 3.9, 3.10, Add examples	Hanjun.Liu

Scope

This document presents the AT command of SSL operation and application examples. This document can apply to SIM800 series modules, including SIM800, SIM800-WB64, SIM800H without blultooth function and SIM800G.

1. SSL Function

1.1. SSL Description

Secure socket layer (SSL), a security protocol, is first put forward by Netscape at the same time as they lunch the first version of Web Browser, the purpose is to provide security and data integrity for network communication. SSL encrypts network connection at the transport layer.

SSL uses public key technology to ensure the confidentiality and reliability of communication between applications, so that the communication between client and server application will not be intercepted by the aggressor. It can be supported on both the server and the client ends, has become the industry standard secure communication on the internet. The current Web browsers generally combine the HTTP and SSL, enabling secure communication. This Agreement and its successor is TLS (Transport Layer Security).

TLS using the key algorithm provided endpoint authentication and secure communication on the Internet, which is based on public key infrastructure (PKI). However, in the example of a typical implementation, only the network service provider is reliable authentication, the client is not necessarily. This is because the public key infrastructure common in commercial operation, electronic signature certificate is usually required to pay for. Protocol is designed in a way to make the master-slave architecture application communication itself prevent eavesdropping, tampering, and message forgery.

SIM800 series support SSL2.0, SSL3.0, TLS1.0

1.2. HTTPS Description

HTTPS is the HTTP channel which targets secure, in simple terms is safe version of HTTP. Added layer of SSL below HTTP, security of HTTPS is based on SSL, so the details please see the SSL encryption.

It is a URI scheme (abstract identifier system), syntax similar to http: System. For secure HTTP data transmission. HTTPS:URL shows that it uses HTTP, but HTTPS exists a default port different with HTTP and has an encryption / authentication layer (between HTTP and TCP). This system was originally developed by Netscape for providing authenticated and encrypted communication method, and now it is widely used in security-sensitive communication on the World Wide Web, such as transaction payment.

1.3. FTPS Description

FTPS is a multi-transmission protocol, equivalent to the encrypted version of the FTP. It is an enhanced FTP protocol which uses standard FTP protocol and commands in the Secure Sockets

Layer. It add SSL security features for FTP protocol and data channels. FTPS is also known as "FTP-SSL" and "FTP-over-SSL". SSL is a protocol which encrypts and decrypts data in secure connection between client and an SSL-enabled server.

1.4. EMAIL Encrypted Transmission Description

To receive Email, SIM800 series support SSL encrypted POP3 protocol which is called POP3S. It will use special port, default port: 995. To send Email, SIM800 series use HTTPS communication, default port: 465. SIM800 series also supports the use of ordinary port, through the STARTTLS (SMTP) and STLS (POP3) to enable encryption transmission.

1.5. SSL AT Command

There is a set of AT commands to support SSL operations, including HTTP, EMAIL and FTP function.

2. AT Command

SIM800 series modules provide encrypted link AT command is as follows:

Command	Description
AT+EMAILSSL	Set EMAIL to use SSL function
AT+HTTPSSL	Set HTTP to use SSL function
AT+FTPSSL	Set FTP to use SSL function
AT+CIPSSL	Set TCP to use SSL function
AT+SSLSETCERT	Import SSL certificate file
AT+SSLOPT	SSL option

2.1. AT+EMAILSSL Set Email to Use SSL Function

AT+EMAILSSL Set EMAIL to Use SSL Function	
Test Command **AT+EMAILSSL=?**	Response **+EMAILSSL:** (list of supported **<n>**s) **OK**
	Parameters See Write Command
Read Command **AT+EMAILSSL?**	Response **+ EMAILSSL: <n>** **OK**
	Parameters See Write Command
Write Command **AT+EMAILSSL=<n>**	Response **OK**
	Parameters **<n>** 0 Not use encrypted transmission 1 Begin encrypt transmission with encryption port 2 Begin encrypt transmission with normal port
Reference	Note: An error code will return if the SSL channel setup failure or communication errors happened when sending mail: **+SMTPSEND: <code>** An error code when sign POP3 server: **+POP3IN: <code>** **<code>** 71 SSL failed to establish channels 72 SSL alert message with a level of fatal result in the immediate termination of the connection

2.2. AT+HTTPSSL Set HTTP to Use SSL Function

AT+HTTPSSL Set HTTP to Use SSL Function	
Test Command **AT+HTTPSSL=?**	Response **+HTTPSSL:** (0-1) **OK**
	Parameters See Write Command
Read Command **AT+HTTPSSL?**	Response **+ HTTPSSL: <n>** **OK**
	Parameters See Write Command
Write Command **AT+HTTPSSL=<n** **>**	Response **OK**
	Parameters **<n>** 0 Disable SSL function 1 Enable SSL function
Reference	Note: An error code will return if HTTPACTION command fail: **+HTTPACTION: <code>** **<code>** 605 SSL failed to establish channels 606 SSL alert message with a level of fatal result in the immediate termination of the connection

2.3. AT+FTPSSL Set FTP to Use SSL Function

AT+FTPSSL Set FTP to Use SSL Function	
Test Command **AT+FTPSSL=?**	Response **+FTPSSL:** (0-2) **OK**
	Parameters See Write Command
Read Command **AT+FTPSSL?**	Response **+ FTPSSL: <n>** **OK**
	Parameters

	See Write Command
Write Command **AT+FTPSSL=<n>**	Response **OK**
	Parameters **<n>** 0 Disable SSL function 1 Use FTPS with Implicit mode 2 Use FTPS with Explicit mode
Reference	Note: An error code will return if FTP operation fail, case in FTPGET: **+FTPGET: <code>** **<code>** 80 SSL failed to establish channels 81 SSL alert message with a level of fatal result in the immediate termination of the connection 82 FTP AUTH error 83 FTP PBSZ error 84 FTP PROT error

2.4. AT+CIPSSL Set TCP to Use SSL Function

AT+CIPSSL Set TCP to Use SSL Function	
Test Command **AT+CIPSSL=?**	Response **+CIPSSL:** (0-1) **OK**
	Parameters See Write Command
Read Command **AT+CIPSSL?**	Response **+ CIPSSL: <n>** **OK**
	Parameters See Write Command
Write Command **AT+CIPSSL=<n>**	Response **OK**
	Parameters **<n>** 0 Disable SSL function 1 Enable SSL function
Reference	Note: ● After set AT+CIPSSL=1, module will automatic begin SSL certificate after TCP connected ● Currently, we just support SSL Client function.

2.5. AT+SSLSETCERT Import SSL Certificate File

AT+SSLSETCERT	Import SSL Certificate File
Test Command **AT+SSLSETCERT=?**	Response **+SSLSETCERT:** max length of field **<file>,**max length of field **<password>** **OK**
Write Command **AT+SSLSETCERT=<file>[,<password>]**	Response **OK** If import succeed **+SSLSETCERT: 0** If import failed **+SSLSETCERT: 1**
	Parameters **<file>** file to be imported. Alphanumeric ASCII text string up to 100 characters. **<password>** password required to parse the certificate file. Alphanumeric ASCII text string up to 32 characters.
Reference	Note: ● Just one file can be imported. If import more than once, module will keep last imported file. ● Support ".crt" or ".cer" certificate file.

2.6. AT+SSLOPT SSL Option

AT+SSLOPT	SSL Option
Test Command **AT+SSLOPT=?**	Response **+SSLOPT: (**range of **<opt>**s**),(**range of **<enable>**s**)** **OK**
	Parameters See Write Command
Read Command **AT+SSLOPT?**	Response **+SSLOPT: 0,<enable>** **+SSLOPT: 1,<enable>** **OK**
	Parameters See Write Command
Write Command	Response

AT+SSLOPT=<opt>,<enable>	**OK**
	Parameters **<opt>** 0 ignore invalid certificate 1 client authentication **<enable>** 0 close 1 open
Reference	Note: The option “client authentication” had not be implement

3. Examples

The following table provides some using method of the SSL function.

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

3.1. EMAIL Send Encrypted Mail with Normal Port

Grammar	Description
AT+SAPBR=3,1,"APN","CMNET" OK	Configure bearer profile 1
AT+SAPBR=1,1 OK	To open a GPRS context.
AT+EMAILCID=1 OK	Set EMAIL Use bear profile 1
AT+EMAILTO=30 OK	Set EMAIL timeout
AT+EMAILSSL=2 OK	Set EMAIL begin encrypt transmission with normal port
AT+SMTPSRV="SMTP.GMAIL.COM" OK	Set SMTP server address, port is omitted, means use the default ports: 25
AT+SMTPAUTH=1,"account","password" OK	Set user name and password
AT+SMTPFROM="account@GMAIL.COM","account" OK	Set sender address and name
AT+SMTPSUB="Test" OK	Set the subject
AT+SMTPRCPT=0,0, "john@sim.com","john" OK	Set the recipient (To:)
AT+SMTPBODY=19 DOWNLOAD This is a new Email OK	Set the body
AT+SMTPSEND OK +SMTPSEND: 1	Send the Email

3.2. EMAIL Send Encrypted Mail with Encryption Port

Grammar	Description
AT+SAPBR=3,1,"APN","CMNET" OK	Configure bearer profile 1
AT+SAPBR=1,1 OK	To open a GPRS context.
AT+EMAILCID=1 OK	Set EMAIL Use bear profile 1
AT+EMAILTO=30 OK	Set EMAIL timeout
AT+EMAILSSL=1 OK	Set EMAIL begin encrypt transmission with encryption port
AT+SMTPSRV="SMTP.GMAIL.COM" OK	Set SMTP server address, port is omitted, means use the default ports: 465
AT+SMTPAUTH=1,"account","password" OK	Set user name and password
AT+SMTPFROM="account@GMAIL.COM","account" OK	Set sender address and name
AT+SMTPSUB="Test" OK	Set the subject
AT+SMTPRCPT=0,0, "john@sim.com","john" OK	Set the recipient (To:)
AT+SMTPBODY=19 DOWNLOAD This is a new Email OK	Set the body
AT+SMTPSEND OK +SMTPSEND: 1	Send the Email

3.3. EMAIL Receive Encrypted Mail with Normal Port

Grammar	Description
AT+SAPBR=3,1,"APN","CMNET" OK	Configure bearer profile 1
AT+SAPBR=1,1 OK	To open a GPRS context.
AT+EMAILCID=1 OK	Set EMAIL Use bear profile 1

AT+EMAILTO=30 OK	Set EMAIL timeout
AT+EMAILSSL=2 OK	Set EMAIL begin encrypt transmission with normal port
AT+POP3SRV="mail.sim.com","john","123456" OK	Set POP3 server and account, port is omitted, means use the default ports 110
AT+POP3IN OK +POP3IN: 1	Log in POP3 server
AT+POP3NUM OK +POP3NUM: 1,2,11124	Get Email number and total size
AT+POP3LIST=1 OK +POP3LIST: 1,1,5556	Get the specific Email’s size
AT+POP3CMD=4,1 OK +POP3CMD: 1	Retrieve the specific Email
AT+POP3READ=1460 +POP3READ: 1,1460 … OK AT+POP3READ=1460 +POP3READ: 1,1460 … OK	Get the Email content
AT+POP3READ=1460 +POP3READ: 2,1183 … OK	The Email’s content is read completely
AT+POP3OUT OK +POP3OUT: 1	Log out POP3 SERVER

3.4. EMAIL Receive Encrypted Mail with Encryption Port

Grammar	Description
AT+SAPBR=3,1,"APN","CMNET" OK	Configure bearer profile 1
AT+SAPBR=1,1 OK	To open a GPRS context.
AT+EMAILCID=1 OK	Set EMAIL Use bear profile 1
AT+EMAILTO=30 OK	Set EMAIL timeout
AT+EMAILSSL=1 OK	Set EMAIL begin encrypt transmission with encryption port
AT+POP3SRV="mail.sim.com","john","123456" OK	Set POP3 server and account, port is omitted, means use the default ports 995
AT+POP3IN OK +POP3IN: 1	Log in POP3 server
AT+POP3NUM OK +POP3NUM: 1,2,11124	Get Email number and total size
AT+POP3LIST=1 OK +POP3LIST: 1,1,5556	Get the specific Email’s size
AT+POP3CMD=4,1 OK +POP3CMD: 1	Retrieve the specific Email
AT+POP3READ=1460 +POP3READ: 1,1460 … OK AT+POP3READ=1460 +POP3READ: 1,1460 … OK	Get the Email content
AT+POP3READ=1460	The Email’s content is read completely

+POP3READ: 2,1183 … OK	
AT+POP3OUT OK +POP3OUT: 1	Log out POP3 SERVER

3.5. HTTPS Get Method with HTTPS

Use HTTPS download data from HTTP server.

Grammar	Description
AT+HTTPINIT OK	Init HTTP service
AT+HTTPPARA="CID",1 OK AT+HTTPPARA="URL","www.gmail.com" OK AT+HTTPPARA ="REDIR",1 OK	Set parameters for HTTP session
AT+HTTPSSL=1 OK	Enable HTTPS function
AT+HTTPACTION=0 OK +HTTPACTION: 0,200,84200	GET session start GET successfully
AT+HTTPREAD +HTTPREAD: 84200 …. OK	Read the data of HTTP server
AT+HTTPTERM OK	Terminate HTTP service

3.6. FTP Get Method with Implicit FTPS

Use Implicit FTPS mode download data from FTP server

Grammar	Description
AT+FTPCID=1 OK AT+FTPSERV="116.228.221.52" OK AT+FTPUN="sim.cs1" OK AT+FTPPW="******" OK AT+FTPGETNAME="1K.txt" OK AT+FTPGETPATH="/" OK	Set parameters for FTP session.
AT+FTPSSL=1 OK	Open Implicit FTPS mode
AT+FTPGET=1 OK	Open the FTP get session.
+FTPGET: 1,1	Data are available.
AT+FTPGET=2,1024 +FTPGET: 2,50 01234567890123456789012345678901234567890123456789 OK	Request to read 1024 bytes, but Only 50 bytes are now available.
AT+FTPGET=2,1024 +FTPGET: 2,0 OK +FTPGET: 1,1	Request to read 1024 bytes again. No byte is now available, but it is not the end of session. If the module receives data but user do not input “AT+FTPGET:2, <reqlength>” to read data, “+FTPGET:1,1” will be shown again in a certain time.
AT+FTPGET=2,1024 +FTPGET: 2,1024 01234567890123456789012345678901234567890…..1234 OK	Request to read 1024 bytes. 1024 bytes are now available.
+FTPGET:1,0	Data transfer finished. The connection to the FTP server is closed.

3.7. FTP Get Method with Explicit FTPS

Use Explicit FTPS mode download data from FTP server

Grammar	Description
AT+FTPCID=1 OK AT+FTPSERV="116.228.221.52" OK AT+FTPUN="sim.cs1" OK AT+FTPPW="******" OK AT+FTPGETNAME="1K.txt" OK AT+FTPGETPATH="/" OK	Set parameters for FTP session.
AT+FTPSSL=2 OK	Open Explicit FTPS mode
AT+FTPGET=1 OK +FTPGET: 1,1	Open the FTP get session. Data are available.
AT+FTPGET=2,1024 +FTPGET: 2,50 01234567890123456789012345678901234567890123456789 OK	Request to read 1024 bytes, but Only 50 bytes are now available.
AT+FTPGET=2,1024 +FTPGET: 2,0 OK +FTPGET: 1,1	Request to read 1024 bytes again. No byte is now available, but it is not the end of session. If the module receives data but user do not input “AT+FTPGET:2, <reqlength>” to read data, “+FTPGET:1,1” will be shown again in a certain time.
AT+FTPGET=2,1024 +FTPGET: 2,1024 01234567890123456789012345678901234567890…..1234 OK +FTPGET:1,0	Request to read 1024 bytes. 1024 bytes are now available. Data transfer finished. The connection to the FTP server is closed.

3.8. Establish a TCP Client Connection over SSL

Grammar	Description
AT+CGATT? +CGATT: 1 OK	GPRS Service's status
AT+CSTT="CMNET" OK	Start task and set APN. The default APN is "CMNET", with no username or password. Check with local GSM provider to get the APN.
AT+CIICR OK	Bring up wireless connection (GPRS or CSD)
AT+CIFSR 10.78.245.128	Get local IP address
AT+CIPSSL=1 OK	Enable SSL function
AT+CIPSTART="TCP","116.228.221.51","8500" OK CONNECT OK	Start up the connection The TCP connection has been established successfully. SSL certificate finished.
AT+CIPSEND > hello TCP serve SEND OK hello SIM800 CLOSED	Send data to remote server, CTRL+Z (0x1a) to send. User should write data only after the promoting mark ">" , and then use CTRL+Z to send. User can use command "AT+CIPSPRT" to set whether echo promote ">" after issuing "AT+CIPSEND". Remote server receives data. For TCP, "SEND OK" means data has been sent out and received successfully by the remote server, due to the TCP connection-oriented protocol; Received data from remote server Remote server closed the connection

3.9. Establish a TCP Client Connection over SSL in Multi Connection

AT+CIPSSL=1 must be set first if customer want to start a TCP connection over SSL. Any TCP connection established before AT+CIPSSL=1 will not try SSL certificate.

Grammar	Description
AT+CGATT? +CGATT: 1	GPRS Service's status

OK	
AT+CIPMUX=1 OK	Enable multi connection
AT+CSTT="CMNET" OK	Start task and set APN.
AT+CIICR OK	Bring up wireless connection (GPRS r CSD)
AT+CIFSR 10.78.245.128	Get local IP address
AT+CIPSTART=0, "TCP","116.228.221.51","8500" OK 0, CONNECT OK	Establish a TCP connection, connection number 0
AT+CIPSSL=1 OK	Enable SSL function. Connection 0 will not start SSL certificate
AT+CIPSTART=1, "TCP","116.228.221.51","9600" OK 1, CONNECT OK	Establish a TCP connection, connection number 1. SSL certificate finished.
AT+CIPSEND=0 > TCP test 0, SEND OK	Send data to connection 0
AT+CIPSEND=1 > TCP Over SSL test 1, SEND OK +RECEIVE,0,17: SIM800 TCP test +RECEIVE,1,26: SIM800 TCP Over SSL test 0, CLOSED	Send data to connection 1 Received data from connection 0, data length 17 Received data from connection 1, data length 26 Connection 0 is closed by remote server
AT+CIPSTATUS OK STATE: IP PROCESSING C: 0,0,"TCP","116.228.221.51","8500"," CLOSED " C: 1,0,"TCP","116.228.221.51","9600"," CONNECTED " C: 2,,"","","","INITIAL" C: 3,,"","","","INITIAL"	Query the current connection status

C: 4,,"","","","INITIAL" C: 5,,"","","","INITIAL"	

3.10. Import a SSL Certificate File

Grammar	Description
AT+FSCREATE=C:\USER\HENRY_SSL.CRT OK	Create certificate file on FS.
AT+FSWRITE=C:\USER\HENRY_SSL.CRT,0,1196,10 > OK	Write file to FS.
AT+SSLSETCERT="C:\USER\HENRY_SSL.CRT","********" OK +SSLSETCERT: 0	Import certificate file Import succeed

Appendix

A. Related Documents

SN	Document name	Remark
[1]	SIM800 Series AT Command Manual	

B. Terms and Abbreviations

Abbreviation	Description
URC	Unsolicited request code
TE	Terminal Equipment
TA	Terminal Adapter
DTE	Data Terminal Equipment or plainly "the application" which is running on an embedded system
DCE	Data Communication Equipment or facsimile DCE(FAX modem, FAX board)
ME	Mobile Equipment
MS	Mobile Station
SSL	Secure Socket Layer
TLS	Transport Layer Security

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 3020
URL: www.sim.com/wm