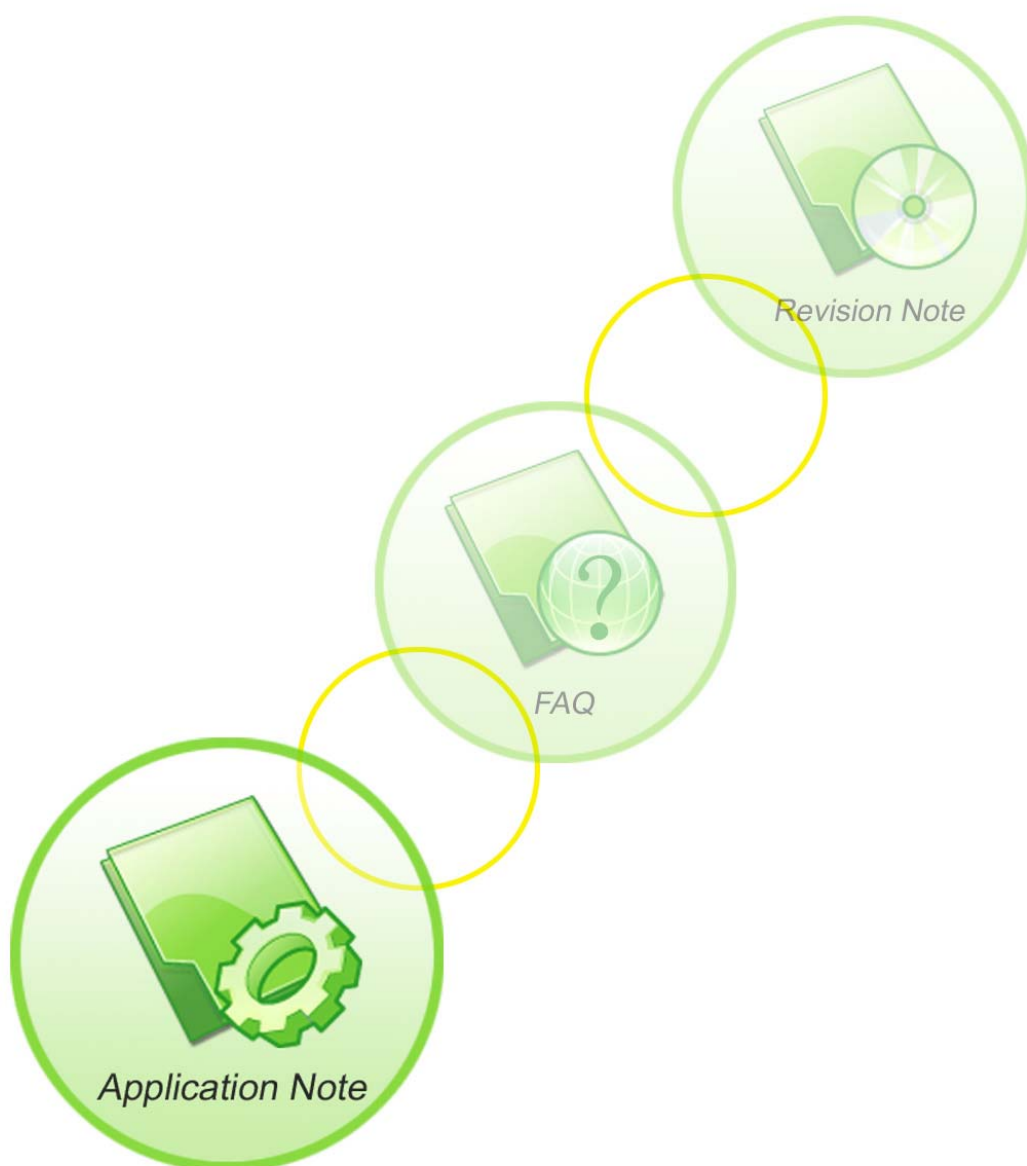




A company of SIM Tech

SIM800 Series_SSL_Application Note_V1.00



Document Title:	SIM800 Series_SSL_Application Note
Version:	1.00
Date:	2013-09-18
Status:	Release
Document Control ID:	SIM800 Series_SSL_ Application Note_V1.00

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 Shanghai SIMCom Wireless Solutions Ltd, 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

Contents

1. SSL Function	5
1.1. SSL Description	5
1.2. HTTPS Description	5
1.3. FTPS Description	5
1.4. EMAIL Encrypted Transmission Description	6
1.5. SSL AT Command	6
2. AT Command	7
2.1. AT+EMAILSSL Set Email to Use SSL Function	7
2.2. AT+HTTPSSL Set HTTP to Use SSL Function	8
2.3. AT+FTPSSL Set FTP to Use SSL Function	8
3. Examples	10
3.1. EMAIL Send Encrypted Mail with Normal Port	10
3.2. EMAIL Send Encrypted Mail with Encryption Port	11
3.3. EMAIL Receive Encrypted Mail with Normal Port	11
3.4. EMAIL Receive Encrypted Mail with Encryption Port	13
3.5. HTTPS Get Method with HTTPS	14
3.6. FTP Get Method with Implicit FTPS	15
3.7. FTP Get Method with Explicit FTPS	16
Appendix	17
A. Related Documents	17
B. Terms and Abbreviations	17

Version History

Date	Version	What is new	Author
2013-10-18	1.00	New version	Hanjun.liu

Scope

This document presents the AT command of SSL operation and application examples. This document can apply to SIM800H and SIM800L modules.

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 launch 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.

SIM800H and SIM800L 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 encrypt and decrypt data in secure connection between client and an SSL-enabled server.

1.4. EMAIL Encrypted Transmission Description

To receive Email, SIM800H and SIM800L support SSL encrypted POP3 protocol which is called POP3S. It will use special port, default port: 995. To send Email, SIM800H and SIM800L use HTTPS communication, default port: 465. SIM800H and SIM800L 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

2.1. AT+EMAILSSL Set Email to Use SSL Function

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

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
	Parameter See Write Command
Read Command AT+HTTPSSL?	Response + HTTPSSL: <n>
	OK
	Parameter See Write Command
Write Command AT+HTTPSSL=<n> >	Response OK
	Parameter <n> <u>0</u> 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
	Parameter See Write Command
Read Command AT+FTPSSL?	Response + FTPSSL: <n>
	OK
	Parameter See Write Command

<p>Write Command AT+FTPSSL=<n></p>	<p>Response OK</p> <p>Parameter</p> <p><n> <u>0</u> Disable SSL function 1 Use FTPS with Implicit mode 2 Use FTPS with Explicit mode</p>
<p>Parameter</p>	<p>Note:</p> <p>An error code will return if FTP operation fail, case in FTPGET: +FTPGET: <code></p> <p><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</p>

SIMCOM CONFIDENTIAL

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+HTTPIPINIT OK	Init HTTP service
AT+HTTTPARA = "CID",1 OK AT+HTTTPARA="URL","www.gmail.com" OK AT+HTTTPARA = "REDIR",1 OK	Set parameters for HTTP session
AT+HTTSSL=1 OK	Enable HTTPS function
AT+HTTTPACTION=0 OK +HTTTPACTION: 0,200,84200	GET session start GET successfully
AT+HTTTPREAD +HTTTPREAD: 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="/"	Set parameters for FTP session.
AT+FTPSSL=1 OK	Open Implicit FTPS mode
AT+FTPGET=1 OK +FTPGET: 1,1	Open the FTP get session. Data are available.
AT+FTPGET=2,1024 +FTPGET: 2,50 012345678901234567890123456789012345678901 23456789 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, “+FTPGE T:1,1” will be shown again in a certain time.
AT+FTPGET=2,1024 +FTPGET: 2,1024 012345678901234567890123456789012345678901 234567890.....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.

3.7. 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="/"	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 012345678901234567890123456789012345678901 23456789 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, “+FTPGE T:1,1” will be shown again in a certain time.
AT+FTPGET=2,1024 +FTPGET: 2,1024 012345678901234567890123456789012345678901 234567890.....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.

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

SIMCOM CONFIDENTIAL FILE