A company of SIM Tech

SIM7000 series_ SSL_ Application Note _V1.00

Title	SIM7000 series _SSL_ Application Note
Version	1.00
Date	2018-04-16
Status	Released/Confidential
Document Control No.	SIM7000 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 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.

Copyrights

Catalog

Version History

Date	Version	Revision Description	Author
2018-04-16	1.00	First release	

1 SSL Function

1.1 SSL Introduction

Secure Sockets Layer，SSL，a security protocol, It was proposed by Netscape at the same time as the first version of the Web browser to provide security and data integrity for network communications. SSL encrypts network connections at the transport layer.

SSL uses public secret key technology to ensure the confidentiality and reliability of communication between two applications, so that communication between client and server applications is not eavesdropped by attackers. It can be supported on both servers and clients at the same time and has become the industry standard for secure communication on the Internet. It is also common for existing Web browsers to combine HTTP and SSL for secure communication. This protocol and its successor are Transport Layer Security (TLS)SSL.

TLS uses secret key algorithms to provide endpoint authentication and communication security on the Internet, based on public key infrastructure (PKI). In a typical example of an implementation, however, only the network service is reliably authenticated, and its clients are not. This is because public key infrastructure is generally commercial, and e-signing certificates are usually purchased for a fee. The protocol is designed in part to enable master-slave architecture applications to communicate themselves to prevent eavesdropping, interference, and message counterfeiting TLS

SIM7000 series support TLS1.0，TLS1.1，TLS1.2，DTLS1.0，DTLS1.2.

2 AT command for TCP/UDP that support SSL

AT command for device use provided by module as follows:

Command	Description
AT+CACID	Setup TCP/UDP identification
AT+CASSL	Setup protocol type and SLL configuration identification
AT+CASSLCFG	Setup SSL certificate and timeout
AT+CAOPEN	Open one TCP/UDP connection
AT+CASEND	Send data
AT+CARECV	Receive data
AT+CACLOSE	Close one TCP/UDP connection
AT+CSSLCFG	Configure SLL parameter

3 Testing Case

3.1 Establish a common TCP/UDP connection

Grammar	State
AT+CNACT=1,"cmnet" OK +APP PDP: ACTIVE AT+CNACT? +CNACT: 1,"10.181.182.177" OK	Open wireless connection, the parameter cmnt setup as APN, this parameter need be setup as different APN value according to different SIM card. Get local IP
AT+CACID=0 OK	Device identification
AT+CASSL=0,0,0 OK	Setup protocol type The first parameter is the corresponding identification. The second parameter is if use SLL, if it is common TCP/UDP connection, the parameter is 0. The third parameter is protocol type, 0 setup here is TCP. If it is UDP, the parameter need be setup as 1, means AT+CASSL=0,0,1 is common UDP protocol.
AT+CAOPEN=0,"116.247.119.165",5171 +CAOPEN: 0,0 OK	Setup a TCP connection Return URC the first parameter is identification, the second parameter is the result of setup connection, 0 is connection success.
AT+CASEND=0,5 > OK +CASEND: 0,0,5	Request to send 5 bytes data Input data Data transmit success
AT+CARECV=0,100 +CARECV: 0,20 GFDSGFDGFDSGHFDSHFDS OK	Request to get 100 bytes data sending from server. In fact, receive 20 bytes data Output data received

AT+CACLOSE=0 OK	Close the connection of Identification 0
AT+CNACT=0 OK +APP PDP: DEACTIVE	Disconnect the wireless connection

3.2 Establish a SLL connection

When establishing a communication, SSL needs to verify the identity of both parties, including one-way certificate and two-way certificate.

One-way certificate is the client to validate the server's certificate. The server sends its own server certificate to the client, the client can verify whether the root of the server certificate issued certificate can be trusted, if you can trust will continue the following communication process.

Two-way certificate client authentication server certificate, the client needs to send your certificate to the server, for server to verify your client certificate. The validation process is the same, and you need to verify that the root certificate that issued the certificate can be trusted SSL Setup a one-way SLL connection

Since the module can only be used as a client at present, when a one-way authentication connection needs to be established, the server's root certificate needs to be imported. If no certificates are imported, the module defaults to all servers being trusted.

Grammar	State
AT+CNACT=1,"cmnet" OK +APP PDP: ACTIVE AT+CNACT? +CNACT: 1,"10.181.182.177" OK	Open wireless connection, the parameter cmnt setup as APN, this parameter need be setup as different APN value according to different SIM card. Get local IP
AT+CACID=0 OK	Device identification
AT+CSSLCFG="sslversion",0,1 OK	Setup identification as 0 SLL protocol type 1 is TLS1.0
AT+CASSL=0,1,0 OK	Setup Protocol type The first parameter is the corresponding identification. The second parameter is if use SLL, 1 is open SLL function.

	The third parameter is AT+CSSLCFG corresponding SLL configuration identification.
AT+CASSLCFG=0,"cacert","root.pem" OK	Setup root certificate, this root certificate must be the certificate switched by AT+CSSLCFG. This can be omitted if all server certificates are trusted by default.
AT+CAOPEN=0,"116.247.119.165",5171 +CAOPEN: 0,0 OK +CARECV: 0,38	Setup a SLL connection Connection setup success Receive 38 bytes data, after establishing connection or sending data successful, the module will take the initiative to read a data. If received the server data, it will report the URC, if not receive the data, it will not report the URC.
AT+CARECV=0,100 +CARECV: 0,38 220 Serv-U FTP Server v15.0 ready... OK	Read 100 bytes data In fact, receive 38 bytes data Output data
AT+CACLOSE=0 OK	Close the connection of identification 0
AT+CNACT=0 OK +APP PDP: DEACTIVE	Disconnect the wireless connection

3.2.2 Establish a SLL connection of two-way certificate

Establish a two-way authenticated SSL connection requires setting up the client certificate. The client certificate needs to be converted through AT+CSSLCFG first. Module can support certificate format is. PEM,, DER, P7B.

Grammar	State
AT+CNACT=1,"cmnet" OK +APP PDP: ACTIVE	Open wireless connection, the parameter cmnt setup as APN, this parameter need be setup as different APN value according to different SIM card.
AT+CNACT? +CNACT: 1,"10.181.182.177"	Get local IP

OK	
AT+CACID=0 OK	Device identification
AT+CSSLCFG="sslversion",0,1 OK	Setup identification as 0 SLL protocol type 1 is TLS1.0
AT+CASSL=0,1,0 OK	Setup Protocol type The first parameter is the corresponding identification. The second parameter is if use SLL, 1 is open SLL function. The third parameter is AT+CSSLCFG corresponding SLL configuration identification.
AT+CASSLCFG=0,"cacert","root.pem" OK	Setup root certificate, this root certificate must be the certificate switched by AT+CSSLCFG. This can be omitted if all server certificates are trusted by default.
AT+CASSLCFG=0,"clientcert","client.pem" OK	Establish client certificate, This client certificate must be the certificate switched by AT+CSSLCFG.
AT+CAOPEN=0,"116.247.119.165",5171 +CAOPEN: 0,0 OK	Establish a SLL connection Connection setup success
AT+CASEND=0,5 > OK +CASEND: 0,0,5	Request to send 5 bytes data Input data Data sending success
AT+CACLOSE=0 OK	Close the connection of identification 0
AT+CNACT=0 OK +APP PDP: DEACTIVE	Disconnect the wireless connection

3.2.3 Use AT+CSSLCFG switch SSL certificate

AT+CSSLCFG="convert",2,"root.pem" OK	Configure the certificate type which need be switched. 2 is the root certificate configuration need to transform the certificate name, after the

	success of the transformation, the name must be same as the name of the existing certificate.
AT+CSSLCFG="convert",1,"client.pem","client.key” OK	Configure the certificate type which need be switched, 1 is the client certificate configuration need to transform the certificate name. Clint certificate need input the certificate file and private key file. After the success of the transformation, the name must be same as the certificate name, it is “client.pem”

Appendix

A. Related documents

Item	Document name	State
[1]	SIM7000 Series AT Command Manual	

B. Conventions and Abbreviations

Conventions	Description
SSL	Secure Sockets Layer，SSL
TLS	Transport Layer Security