imei

SIM7020 Series_TLS _Application Note

LPWA Module

SIMCom Wireless Solutions Limited
Building B, SIM Technology Building, No.633, Jinzhong Road
Changning District, Shanghai P.R. China
Tel: 86-21-31575100
support@simcom.com
www.simcom.com

Document Title:	SIM7020 Series_TLS_Application Note
Version:	1.03
Date:	2020.6.10
Status:	Release

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

SIMCom Wireless Solutions Limited
Building B, SIM Technology Building, No.633 Jinzhong Road, Changning District, Shanghai P.R. China
Tel: +86 21 31575100
Email: simcom@simcom.com

For more information, please visit:
https://www.simcom.com/download/list-863-en.html

For technical support, or to report documentation errors, please visit:
https://www.simcom.com/ask/ or email to: support@simcom.com

About Document

Version History

Version	Date	Owner	What is new
V1.00	2018.4.12	Chengliang.Wang	First Release
V1.01	2018.6.8	Ruihu.Yu	
V1.02	2019.12.10	Chengliang.Wang	Add DTLS Application
V1.03	2020.6.10	Wenjie.Lai	All

Scope

This document applies to the following products

Name	Type	Size（mm）	Comments
SIM7020C	NB1	17.6*15.7	Band 1/3/5/8
SIM7020E	NB1	17.6*15.7	Band 1/3/5/8/20/28
SIM7030	NB1	16*18	Band 1/3/5/8
SIM7060	NB1+GNSS	24*24	Band 5/8
SIM7020G	NB2	17.6*15.7	Band 1/2/3/4/5/8/12/13/17/18/19/20/25/26/28/66/70/71/85
SIM7060G	NB2+GNSS	24*24	Band 1/2/3/4/5/8/12/13/17/18/19/20/25/26/28/66/70/71/85

Contents

1 Introduction

1.1 Purpose of the document

Based on module AT command manual, this document will introduce TLS application process.
Developers could understand and develop application quickly and efficiently based on this document.

1.2 Related documents

[1] SIM7020 Series_AT Command Manual

1.3 Conventions and abbreviations

In this document, the GSM engines are referred to as following term:
ME (Mobile Equipment);
MS (Mobile Station);
TA (Terminal Adapter);
DCE (Data Communication Equipment) or facsimile DCE (FAX modem, FAX board);

In application, controlling device controls the GSM engine by sending AT Command via its serial interface.
The controlling device at the other end of the serial line is referred to as following term:
TE (Terminal Equipment);
DTE (Data Terminal Equipment) or plainly "the application" which is running on an embedded system;

2 TLS Introduction

SSL (Secure Sockets Layer), a security protocol. It was put forward by Netscape in the first version of Web browser. The aim is to provide security and data integrity for network communications. SSL encrypts the network connections at the transport layer.

SSL uses public key technology to ensure the confidentiality and reliability of communication between two applications and to ensure that communication between client and server applications is not eaves dropped by attackers. It can be supported at both ends of the server and client, and has become an industrial standard for secure communication over the Internet. Current Web browsers generally combine HTTP and SSL to achieve secure communication. This Agreement and its successor are TLS (Transport Layer Security, TLS).

TLS uses key algorithm to provide endpoint authentication and communication security on the Internet, It is based on the public key infrastructure. In typical implementations, however, only the network server is authenticated reliably, while the client is not necessarily. This is because the public key infrastructure is generally commercial, and electronic signature certificates usually need to be paid for. The protocol is designed to enable master-slave architecture application communication itself to prevent tapping, tampering, and message forgery.

SIM7020 series modules currently support TLS1.0, TLS1.1, TLS1.2.

3 Bearer Configuration

Usually module will register PS service automatically.

3.1 PDN Auto-activation

```
//Example of PDN Auto-activation.

AT+CPIN?                                    // Check SIM card status
+CPIN: READY

OK
AT+CSQ                                      // Check RF signal
+CSQ: 27,99

OK
AT+CGATT?                                   // Check PS service. 1 indicates PS has attached.
+CGATT: 1

OK
AT+CGACT?                                   // PDN active success
+CGACT:1,1

OK
AT+COPS?                                    // Query Network information, operator and network mode 9, NB-IOT network
+COPS:0,0,”CHN-UNICOM”,9

OK
AT+CGCONTRDP                                // Attached PS domain and got IP address automatically
+CGCONTRDP:
1,5,"shnbiot","10.250.0.213.255.255.255.0"

OK
```

3.2 APN Manual configuration

```
//Example of APN Manual configuration.

AT+CFUN=0                                   // Disable RF
+CPIN: NOT READY

OK
AT*MCGDEFCONT="IP","3GNET"                  // Set the APN manually

OK
AT+CFUN=1                                   // Enable RF

OK
+CPIN:READY
AT+CGATT?                                   // Inquiry PS service
+CGATT: 1

OK
AT+CGCONTRDP                                // Attached PS domain and got IP address
+CGCONTRDP:                                 automatically
1,5,"3GNET","10.250.0.253.255.255.255.0"

OK
```

4 TLS Examples

AT+CTLSCFG=1,1,"182.150.27.42",2,50090,3,0,4,0,5,2 **OK**	//Configure TLS server instance, parameters include, <tid>:1 ;<server name>: 1; server ip: 182.150.27.42; <prot>: 2; <port>: 50090; <socket type>:3 for 0 –tcp; <Authentication mode>: 4, value is 0-none; <debug level> : 5, value is 2.
AT+CTLSCFG=1,6,1344,1,"-----BEGIN CERTIFICATE-----\r\nMIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER\r\nMA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN\r\nMTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G\r\nA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G\r\nCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx\r\nmdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny\r\n50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEk" **OK	//Configure TLS server instance, parameters include, <tid>:1 ;<server name>: 1; server ip: 182.150.27.42; <prot>: 2; <port>: 50090; <socket type>:3 for 0 –tcp; <Authentication mode>: 4, value is 0-none; <debug level> : 5, value is 2.
AT+CTLSCFG=1,6,1344,1,"HHxvYPZP9al4jwqj+8n\r\nYMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL\r\nR7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu\r\nKNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj\r\ngZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH\r\n/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV\r\nBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz\r\ndCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIsIsCfdl" **OK	//Configure TLS server instance, parameters include, <tid>:1 ;<server name>: 1; server ip: 182.150.27.42; <prot>: 2; <port>: 50090; <socket type>:3 for 0 –tcp; <Authentication mode>: 4, value is 0-none; <debug level> : 5, value is 2.
AT+CTLSCFG=1,6,1344,0,"c2i94QHHYeJ\r\nSs	//Configure TLS server CA.

R4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMC ZP6C5NyNyXw1GWY/YR82XTJ8H\r\nDBJiCTok 5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d 0IjxM27WNKs4sDQhZBQkF\r\npjmfs2cb4oPl4Y 9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+U shITnmp5/Ztkf\r\nm/UTSLBNFNHesiTZeH31Nc xYGdHSme9Nc/gfidRa0FLOCfWxRIFqAI47zG9j AQCZ\r\n7Z2mCGDNMhjQc+BYcdnl0IPXjdDK6 V0qCg1dVewhUBcW5gZKzV7e9+DpVA==\r\n--- --END CERTIFICATE-----"	No more input after this.
OK	
AT+CTLSCONN=1,1	//Create TLS connection Parameters <tid>: 1 <cid>:1
OK	
AT+CTLSSEND=1,75,"GET https://182.150.27.42/test.html HTTP/1.1\r\nHost: 182.150.27.42\r\n\r\n"	//Send data, parameters <tid>:1 <payload length>: 75 <payload>
OK **+CTLSSEND:1,69**	//URC report <tid>：1 <ret>：69
AT+CTLSRECV=1,100,801	
OK **+CTLSRECV:1,106,"HTTP/1.1 200 OK\r\nDate: Thu, 30 Nov 2017 11:16:24 GMT\r\nServer: Apache/2.4.27 (Win32) OpenSSL/1.0.2l\r\n"**	//Receive data, parameters <tid>:1 <data length>: 100 bytes <code type>: 801 (string)
AT+CTLSCLOSE=1 **OK**	//Terminate TLS connection Parameters, <tid>:1
+CTLSCLOSE:1,1	//URC report: <tid>:1 <ret>:1, means succeed