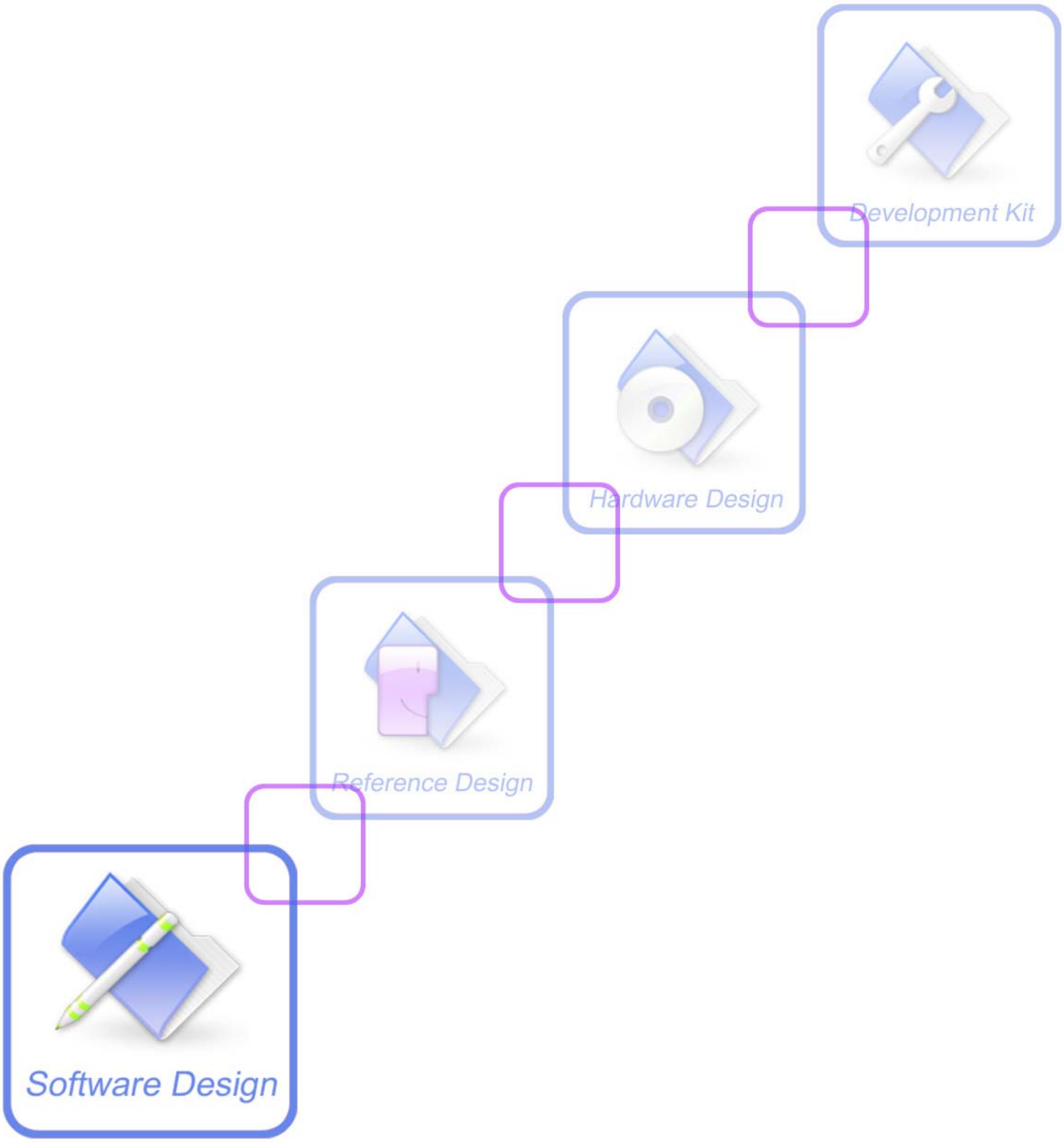
A company of SIM Tech

SIM900 HTTPS AT Commands Set_ V1.00



Document Title:	SIM900 HTTPS AT Commands Set
Version:	1.00
Date:	2012-10-18
Status:	Release
Document Control ID:	SIM900_HTTPS AT Command Set_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

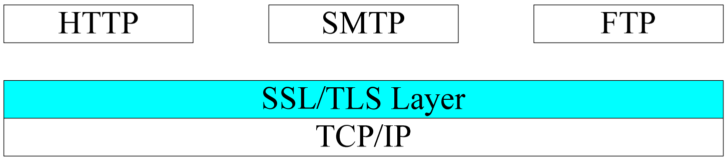
Version History

Version	Chapter	What is new
V1.00	Origin	

1 Introduction

This document presents the AT command of HTTPS operation for SIM900. This document can apply to the same series of the modules which contain HTTPS function, like SIM900, SIM900D, SIM900B and SIM900A.

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. HTTPS is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. The figure is:



SSL/TLS allows an SSL-enabled server to authenticate itself to an SSL-enabled client, and if necessary, allows the client to authenticate itself to the server. After the authentication and cryptology parameter negotiation, a secure channel is established so that the client and server can exchange information in a secure way.

1.1 SSL/TLS Features

- Support SSL 3.0 and TLS 1.0
- Support SSL client only
- Support 512 bits and 1024 bits exportable and non-exportable cipher suits
- Support RSA and Ephemeral Diffie-Hellman key exchange method
- Support RSA(with MD5,SHA1 or MD2) and DSS signature algorithm
- Support Mutual authentication
- Support SSL re-handshake
- Support DES, 3DES, AES, RC2, and ARCFOUR (compatible with RC4) algorithms.
- Support resumed handshake.
- Support user interaction in certificate processing.

1.2 Reference

[1] SIM900_AT Command Manual_V1.06.pdf

1.3 Glossary

IP	Internet Protocol
TCP	Transmission Control Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

2 AT commands

2.1 AT+HTTPSSL

AT+HTTPSSL	**Enable/Disable SSL for HTTP**
Test Command **AT+HTTPSSL=?**	Response **+HTTPSSL:** (list of supported <**mode**>s) **OK**
	Parameter See Write Command
Read Command **AT+HTTPSSL?**	Response **+HTTPSSL: <mode>** **OK**
	Parameter See Write Command
Write Command **AT+HTTPSSL=<mode>**	Response **OK** or **ERROR** or **+CME ERROR: <err>**
	Parameter <**mode**> Integer type. The **<mode>** is used to select whether to enable or disable SSL for HTTP. 0 Disable SSL for HTTP. 1 Enable SSL for HTTP. It can support HTTPS.
Reference	Note

3 Examples

In the following chapter, some examples of HTTPS are given.

NOTE: The website (https://www.example.com) that follows is just as an example, actually it does not exist.

3.1 Bearer Profile

Demonstration	Syntax	Expert Results
Configure bearer profile 1	AT+SAPBR=3,1,"Contype","GPRS" AT+SAPBR=3,1,"APN","CMNET"	OK OK
To open a GPRS context.	AT+SAPBR=1,1	OK
To query the GPRS context	AT+SAPBR=2,1	+SAPBR:1,1,"10.89.193.1" OK
To close the GPRS context.	AT+SAPBR=0,1	OK
GPRS context is released by network		+SAPBR 1: DEACT

3.2 HTTPS Get Method

Demonstration	Syntax	Expert Results
Enable HTTPS	AT+HTTPSSL=1	OK
Init https service	AT+HTTPPARA="CID",1 AT+HTTPPARA="URL","https://www.example.com"	OK OK
GET session start	AT+HTTPACTION=0	OK
GET successfully		+HTTPACTION:0,200,1000
Read the data of HTTPS server	AT+HTTPREAD	+HTTPREAD:1000 … *//output the data to uart*

		OK
Terminate https service	AT+HTTPTERM	OK

3.3 HTTPS POST Method

Demonstration	**Syntax**	**Expert Results**
Enable HTTPS	AT+HTTPSSL=1	OK
Set parameters for HTTPS session	AT+HTTPPARA=”CID”,1 AT+HTTPPARA=”URL”,”https://www.example.com”	OK OK
POST the data whose size is 100 bytes and the maximum latency time for inputting is 10000 ms. It is recommended to set the latency time long enough to download all the data in the latency time	AT+HTTPDATA=100,10000	DOWNLOAD …… *//It is ready to receive data from uart, and DCD has been set to low.* OK *//All data has been Received over, and DCD is set to high.*
POST session start	AT+HTTPACTION=1	OK
POST successfully		+HTTPACTION:1,200,0
Terminate https service	AT+HTTPTERM	OK

3.4 HTTPS HEAD Method

Demonstration	**Syntax**	**Expert Results**
Enable HTTPS	AT+HTTPSSL	OK
Init https service	AT+HTTPINIT	OK
Set parameters for HTTPS session	AT+HTTPPARA=”CID”,1 AT+HTTPPARA=”URL”,”https://www.example.com”	OK OK
HEAD session start	AT+HTTPACTION=2	OK
HEAD successfully		+HTTPACTION:2,200,0

Terminate https service	AT+HTTPTERM	OK

3.5 Set Proxy HTTPS Server

Demonstration	Syntax	Expert Results
Enable HTTPS	AT+HTTPSSL	OK
Init https service	AT+HTTPINIT	OK
Set parameters for HTTPS session	AT+HTTPPARA=”CID”,1 AT+HTTPPARA=”URL”,”https://www.example.com”	OK OK
Set proxy server IP address	AT+HTTPPARA=”PROIP”,”10.0.0.172”	OK
Set proxy server port	AT+HTTPPARA=”PROPORT”,443	OK
GET session start	AT+HTTPACTION=0	OK
GET successfully		+HTTPACTION=0,200,1000
Read the data of HTTPS server	AT+HTTPREAD	+HTTPREAD:1000 … *//output the data to uart* OK
Terminate https service	AT+HTTPTERM	OK

3.6 Set HTTPS Redirection Parameter

Demonstration	Syntax	Expert Results
Enable HTTPS	AT+HTTPSSL	OK
Init https service	AT+HTTPINIT	OK
Set parameters for HTTPS session	AT+HTTPPARA=”CID”,1	OK
Set the redirection parameter	AT+HTTPPARA=”REDIR”,1	OK
Set the wrong URL	AT+HTTPPARA=”URL”,”https://www.example.com/abcde”	OK

GET session start	AT+HTTPACTION=0	OK
GET successfully		+HTTPACTION=0,200,1000
Read the response of HTTPS server	AT+HTTPREAD	+HTTPREAD:1000 … *//output the data to uart* OK
Terminate https service	AT+HTTPTERM	OK

3.7 Set HTTPS Download Break Point Parameter

Demonstration	Syntax	Expert Results
Enable HTTPS	AT+HTTPSSL	OK
Init https service	AT+HTTPINIT	OK
Set parameters for HTTPS session	AT+HTTPPARA=”CID”,1	OK
Set the URL, the size of gif is 16384 bytes	AT+HTTPPARA=”URL”,”https://www.example.com/img/test.gif”	OK
Set the breakpoint	AT+HTTPPARA=”BREAK”,2000	OK
GET session start, get data from 2000 to 16384	AT+HTTPACTION=0	OK
GET successfully		+HTTPACTION=0,200,14384
Read the data of HTTPS server	AT+HTTPREAD	+HTTPREAD:14384 … *//output the data to uart* OK
Terminate https service	AT+HTTPTERM	OK

4 HTTPS URL

Below are HTTPS URLs:

https://accounts.google.com

https://registeronce.autodesk.com

https://support.cdmatech.com/login/

Contact us:

Shanghai SIMCom Wireless Solutions Ltd

Addr: Building A, SIM Technology Building, No.633, Jinzhong Road, Changning Disdrict, Shanghai P.R. China 200355
Tel: +86 21 3252 3300
Fax: +86 21 3252 3020
URL: www.sim.com/wm