

<b>Document Title:</b>	SIM 5360 SSL Application Note
<b>Version:</b>	0.01
<b>Date:</b>	2014-02-24
<b>Status:</b>	Developing
<b>Document ID:</b>	SIM5360_SSL_Application_Note_V0.01

**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**

This document contains proprietary technical information which is the property of SIMCOM Limited., 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*

## Version History

Version	Chapter	Comments
V0.01	New Version	

# Contents

<b>Version History</b> .....	2
<b>Contents</b> .....	3
1. Introduction.....	5
1.1 Overview .....	5
1.2 References .....	5
1.3 Terms and Abbreviations .....	5
2. HTTPS operations.....	5
2.1 Acquire HTTPS stack.....	5
2.2 Connect HTTPS server.....	5
2.3 Send HTTPS Request.....	5
2.4 Receive HTTPS response.....	6
2.5 Close HTTPS connection .....	7
2.6 Release HTTPS stack .....	7
2.7 Timer values of HTTPS operation.....	7
3. FTPS operations.....	7
3.1 Acquire FTPS stack.....	7
3.2 Login the FTPS server.....	8
3.3 Get Current directory on FTPS server.....	8
3.4 Change Current directory on FTPS server .....	8
3.5 Create a new directory on FTPS server.....	8
3.6 Remove a directory on FTPS server.....	9
3.7 Delete a file on FTPS server.....	9
3.8 Set FTPS transfer type.....	9
3.9 List all items in current directory on FTPS server.....	9
3.10 Put a file from EFS to FTPS server .....	9
3.11 Put a file from external MCU to FTPS server .....	10
3.12 Get a file from FTPS server to EFS.....	10
3.13 Get a file from FTPS server to external MCU.....	11
3.14 Logout the FTPS server.....	11
3.15 Release the FTPS stack .....	11
3.16 Timer values of FTPS operation.....	11
4. Common Channel operations.....	12
4.1 Set sending URC and receive data mode.....	12
4.2 Acquire Common Channel stack .....	12
4.3 Open the channel .....	12
4.4 Send data .....	13
4.5 Receive data .....	13
4.6 Close the channel .....	14
4.7 Release the stack .....	14
4.8 Using Transparent Mode for Common Channel Service.....	14
4.9 Timer values of Channel operation.....	15
5. Unsolicited Result Code.....	15

- 5.1 Unsolicited result code of HTTPS..... 15
- 5.2 Unsolicited result code of common channel..... 15
- 6. Certificate & Key Management ..... 15
  - 6.1 Download certificate & key files to the module ..... 16
  - 6.2 List all certificate & key files in the module ..... 16
  - 6.3 Delete a certificate or key file in the module..... 16
  - 6.4 Set the CA file ..... 16
  - 6.5 Set the certificate file..... 17
  - 6.6 Set the key file..... 17
  - 6.7 Load the CA/certificate/key files..... 17
- 7. AT Command Samples..... 17
  - 7.1 AT Command Samples of HTTPS..... 17
  - 7.2 AT Command Samples of FTPS..... 18
  - 7.3 AT Command Samples of Common Channel..... 20
  - 7.4 AT Command Samples of HTTPS supporting cert/key ..... 21
  - 7.5 AT Command Samples of Common Channel supporting cert/key ..... 22
- 8. Conflict AT Commands..... 23

# 1. Introduction

## 1.1 Overview

This document gives the usage of SIM52XX SSL functions; user can get useful information about the SIM52XX SSL functions quickly through this document.

The SSL functions are provided in AT command format, and they are designed for customers to design their HTTPS,FTPS and common SSL applications easily. User can access the SSL AT commands through UART/ USB interface which communicates with SIM52XX module.

### **SIM52XX SSL features:**

- Basic HTTPS GET and POST operations.
- Basic FTPS LOGIN, LOGOUT, LIST, DEL, RMD, MKD, GET, PUT operations.
- Basic SSL socket operations.

## 1.2 References

The present document is based on the following documents:

SIMCOM\_SIM5360\_ATC\_EN\_V0.05.doc

## 1.3 Terms and Abbreviations

For the purposes of the present document, the following abbreviations apply:

- AT                    ATtention; the two-character abbreviation is used to start a command line to be sent from TE/DTE to TA/DCE
- EDGE                Enhanced Data GSM Environment
- EGPRS               Enhanced General Packet Radio Service
- FTPS                 File Transfer Protocol over Secure socket Layer
- GPRS                 General Packet Radio Service
- GSM                 Global System for Mobile communications
- HTTPS               Hypertext Transfer Protocol over Secure Socket Layer
- PIN                    Personal Identification Number
- SSL                    Secure Socket Layer
- TA                    Terminal Adaptor; e.g. a data card (equal to DCE)
- TE                    Terminal Equipment; e.g. a computer (equal to DTE)
- UMTS                 Universal Mobile Telecommunications System
- URC                    Unsolicited Result Code
- USIM                 Universal Subscriber Identity Module

- WCDMA            Wideband Code Division Multiple Access

---

## 2. HTTPS operations

The purpose of this section is to help get you start with HTTPS operations.

### 2.1 Acquire HTTPS stack

Each time when user needs to access a new HTTPS URL (AT+CHTTPSOPSE), the HTTPS stack needs to be acquired before the HTTPS operations:

```
AT+CHTTPSSTART
OK
```

### 2.2 Connect HTTPS server

After acquiring the HTTPS stack, user can connect the HTTPS server using the following AT command:

```
AT+CHTTPSOPSE="www.mywebsite.com", 443, 2
OK
```

The last parameter is the server type. Default is 2(HTTPS server). Following are the HTTPS server that supported:

- 1-HTTP server
- 2-HTTPS server with SSL3.0/TLS1.0 supported

### 2.3 Send HTTPS Request

After the HTTPS connection is established successfully. User can send HTTPS request data using the following AT commands:

```
AT+CHTTPSEND=88
>GET / HTTP/1.1
Host: www.mywebsite.com
User-Agent: MY WEB AGENT
Content-Length: 0
```

```
OK
```

When the HTTPS data is large (for example, posting a large file to server), the AT+CHTTPSEND can be used to send the data segmented to multiple parts:

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/517145125130006122>