



HUAWEI MU509-b HSDPA LGA Module  
V100R003

## **SSL Application Guide**

Issue 01

Date 2014-10-10

## **Copyright © Huawei Technologies Co., Ltd. 2014. All rights reserved.**

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd. and its affiliates ("Huawei").

The product described in this manual may include copyrighted software of Huawei and possible licensors. Customers shall not in any manner reproduce, distribute, modify, decompile, disassemble, decrypt, extract, reverse engineer, lease, assign, or sublicense the said software, unless such restrictions are prohibited by applicable laws or such actions are approved by respective copyright holders.

## **Trademarks and Permissions**



HUAWEI, HUAWEI, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned may be the property of their respective owners.

## **Notice**

Some features of the product and its accessories described herein rely on the software installed, capacities and settings of local network, and therefore may not be activated or may be limited by local network operators or network service providers.

Thus, the descriptions herein may not exactly match the product or its accessories which you purchase.

Huawei reserves the right to change or modify any information or specifications contained in this manual without prior notice and without any liability.

## **DISCLAIMER**

ALL CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL HUAWEI BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOSS OF PROFITS, BUSINESS, REVENUE, DATA, GOODWILL SAVINGS OR ANTICIPATED SAVINGS REGARDLESS OF WHETHER SUCH LOSSES ARE FORSEEABLE OR NOT.

THE MAXIMUM LIABILITY (THIS LIMITATION SHALL NOT APPLY TO LIABILITY FOR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH A LIMITATION) OF HUAWEI ARISING FROM THE USE OF THE PRODUCT DESCRIBED IN THIS MANUAL SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMERS FOR THE PURCHASE OF THIS PRODUCT.

## **Import and Export Regulations**

Customers shall comply with all applicable export or import laws and regulations and be responsible to obtain all necessary governmental permits and licenses in order to export, re-export or import the product mentioned in this manual including the software and technical data therein.

## **Privacy Policy**

To better understand how we protect your personal information, please see the privacy policy at <http://consumer.huawei.com/privacy-policy>.



## About This Document

---

### Revision History

Document Version	Date	Chapter	Descriptions
01	2014-10-10		Creation



# Contents

<b>1 Introduction.....</b>	<b>5</b>
1.1 Scope .....	5
1.2 Audience.....	5
1.3 CyaSSL .....	5
<b>2 Preliminary Operations.....</b>	<b>6</b>
2.1 IP Configuration.....	6
2.2 Configuring or Activating Context.....	6
2.3 SSL.....	7
2.3.1 Cipher Suites .....	8
2.3.2 Certificates.....	8
<b>3 Configure SSL.....</b>	<b>9</b>
3.1 Initialize SSL Library.....	9
3.2 Enable Secure CyaSSL Channel .....	9
3.3 Configure CyaSSL Socket.....	10
3.4 Manage Certificate .....	10
<b>4 Work with SSL.....</b>	<b>18</b>
4.1 Open a Secure Socket .....	18
4.2 Socket Connection Status .....	19
4.3 Exchange Data Through a Secure Socket.....	20
4.3.1 Transmit Data .....	20
4.3.2 Receive Data .....	20
4.4 Close Socket .....	21
<b>5 SSL AT Commands.....</b>	<b>22</b>
<b>6 SSL Error Codes.....</b>	<b>23</b>
<b>7 Abbreviations.....</b>	<b>24</b>



# 1 Introduction

## 1.1 Scope

This document provides the description of the set of Secure Socket Layer (SSL) AT commands related to the SSL protocol.

## 1.2 Audience

This document is intended for people who are about to develop applications using secure sockets.

The reader is expected to have knowledge in wireless technology as well as in AT commands. A basic knowledge of SSL and Transport Layer Security (TLS) security protocol is also needed. For protocol details, refer to [RFC 2246; The TLS Protocol Version 1.0](#).

For details about certificates, refer to [RFC 2459; X509v3](#).

## 1.3 CyaSSL

CyaSSL library is the third party SSL library for building security functionality into embedded devices with minimal footprint and supports SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2 standards. With the help of CyaSSL service layer, application protocols such as HTTPS and Lightweight Directory Access Protocol (LDAP) can be designed to transmit data over a secure connection.



# 2 Preliminary Operations

Before initializing a secure socket and transmitting data over the secure channel, certain preliminary operations need to be performed which are mentioned below.

## 2.1 IP Configuration

CyaSSL requires IP configurations to be done to access the secure server over which data can be transmitted.

## 2.2 Configuring or Activating Context

Before working with AT commands for establishing secure connection using SSL, the activation of a PDP context is needed.

First of all, context parameters have to be set. They consist in a set of information identifying the internet entry point interface provided by the ISP. This can be done using the AT+CGDCONT command:

**AT+CGDCONT[=<cid>[,<PDP\_type>[,<APN>[,<PDP\_addr>[,<d\_comp>[,<h\_com\_p>]]]]]**

Where:

- <cid>: the PDP Context Identifier, a numeric parameter which specifies a particular PDP context definition.
- <PDP\_type>: string value. It indicates the type of the packet switching protocol.  
"IP": IP protocol  
"PPP": Point-to-Point protocol
- <APN>: the Access Point Name, a string that represents logical name used to select GGSN or external packet data network.  
To unlock password protected PIN, use AT+CPIN=<PIN>.
- <PDP\_addr>: string value. It indicates the address of MSI.
- <d\_comp>: a numerical value, controlling the compression of PDP data.  
0: No compression



- 1: Compression
- 2: V.42bi (reserved, not supported currently)  
If no <d\_comp> is included, it is equivalent to the effect that the <d\_comp> is 0.
- <h\_comp>: a numerical value, controlling the compression of PDP header.
  - 0: No compression
  - 1: Compression
  - 2: RFC1144 (applicable for SNDCP only) (reserved, not supported currently)
  - 3: RFC2507 (reserved, not supported currently)
  - Other values are reserved.  
If no <h\_comp> is included, it is equivalent to the effect that the <h\_comp> is 0.

### Example

- To configure APN:  
AT+CGDCONT=1,"IP","mhahuawei1.com"  
OK
- To check the APN settings:  
AT+CGDCONT?  
+CGDCONT: 1,"IP","mhahuawei1.com","",0,0  
  
OK
- To get the signal strength:  
AT+CSQ  
+CSQ: 28,99  
  
OK  
31 is the strongest, 0 is the weakest, and 99 for none.
- To get the registered network:  
AT+COPS?  
+COPS: 0,0,"Terminal MHA Net",2  
  
OK

## 2.3 SSL

SSL is a cryptographic protocol used over the internet to provide secure data communication in client server architecture. Examples are HTTP (HTTPS) connection between web browsers and web servers; SMTP (SMTPTS) connection between SMTP client and server; FTP (FTPS) connection between FTP client and server.



### 2.3.1 Cipher Suites

The cipher suite represents the set of algorithms which are used to negotiate the security settings for a network connection using the SSL network protocol. It includes a public key algorithm (used for sharing the secret key during the handshake), an encryption algorithm (used for encrypting the message stream) and a hash algorithm (used for generating message digests).

The supported cipher suites are listed below:

Value	Cipher_suites
0	All supported Ciphers
1	TLS_RSA_WITH_RC4_128_SHA
2	TLS_RSA_WITH_RC4_128_MD5
3	TLS_RSA_WITH_NULL_SHA
4	TLS_RSA_WITH_NULL_SHA256
5	TLS_RSA_WITH_AES_256_CBC_SHA
6	TLS_RSA_WITH_AES_128_CBC_SHA
7	TLS_RSA_WITH_AES_128_CBC_SHA256
8	TLS_RSA_WITH_AES_256_CBC_SHA256
9	TLS_RSA_WITH_3DES_EDE_CBC_SHA
10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
11	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
12	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
13	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
14	SSL_RSA_WITH_RC4_128_SHA
15	SSL_RSA_WITH_RC4_128_MD5

### 2.3.2 Certificates

The SSL module allows the storage of client and server certificate. The certificates should be in PEM format. Certificates can be stored using AT commands also.



# 3 Configure SSL

Before opening an SSL socket and exchanging data through secure or normal socket, the following steps need to be performed:

- Initialize SSL library
- Enable secure CyaSSL channel
- Configure secure socket
- Manage certificate

## 3.1 Initialize SSL Library

Before opening a secure socket and exchanging data through it, the CyaSSL library needs to be initialized. Once SSL service task is created, CyaSSL library is initialized internally and a CyaSSL context is created.

## 3.2 Enable Secure CyaSSL Channel

The first step to be done in order to exchange data through an SSL socket is to enable the secure socket.

This can be done using the AT command AT^SSLEN:

**AT^SSLEN=<SSL\_id>,<Enable>[,<Encode\_ok>]**

Where:

- <SSL\_id>: must be set to 1, for security socket ID available.
- <Enable>: indicates the desired status. 0 indicates to disable socket; 1 indicates to enable socket.
- <Encode\_ok>: indicates encode type for AT^SSLRX and AT^SSLTX commands (optional, it will take the value as 1 by default).

Without entering this command, any attempt to set SSL parameters by means of an SSL command fails.

### Example

Enable SSL socket 1:



AT^SSLEN=1,1

OK

### 3.3 Configure CyaSSL Socket

CyaSSL socket parameters can be configured using the AT command AT^SSLCFG.

**AT^SSLCFG=<SSL\_id>,<TimeOut>[,cipher\_suit>,security\_level>]**

Where:

- <SSL\_id>: must be set to 1, for security socket ID available.
- <TimeOut>: indicates default maximum blocking timeout. Time out may range from 1s to 60s.
- <cipher\_suit>: set the value to 0; all the available cipher suites supported by CyaSSL are proposed to the server. It is responsibility of the remote server to select one of them. Supported ciphers are mentioned in section 2.3.1 .
- <security\_level>: the authentication mode.
  - 0: SSL verify none: no authentication, no security data is needed at all.
  - 1: Server authentication mode: CA Certificate storage is needed (the most common case).
  - 2: Server or Client authentication mode: CA Certificate (server), Certificate (client) and Private Key (client) are needed.

#### Example

CyaSSL socket configuration:

AT^SSLCFG=1,60,0,1

OK

### 3.4 Manage Certificate

Certificate management can be done using the AT command AT^SSLMNG.

**AT^SSLMNG=<SSL\_id>,<data\_type>,<action>,<file\_name>,[<package\_id>,<total\_no\_of\_packages>,<cert\_info>],[<password>]**

Where:

- <SSL\_id>: should be set to 1 for secure socket.
- <data\_type>: identifies the certificate/key to be stored.
  - 0: Certificate of the client (module).
  - 1: Root CA certificate of the remote server, it is used to authenticate the remote server. It is needed when <security\_level> parameter of AT^SSLCFG command is set to 1 or 2.
  - 2: RSA private key of the client (module). Storing of certificates or private keys are required if the Server or Client authentication mode has been configured. Refer to <security\_level> option in section 3.3 .



- <action>:
  - 0: Store certificate
  - 1: Delete certificate
  - 2: Load certificate
- <file\_name>: the file name used for storing the certificate. The maximum length of the file name is 255.
- <package\_id>: package identification number (1–10).
- <total\_no\_of\_packages>: total number of packages after splitting the Base 64 encoded format certificate data of each package of size maximum of 1024 bytes (1–10).
- <cert\_info>: string type, broken certificate package (converted into Base 64 encoded format before splitting the package) data (1–1024 bytes).  
As we are decoding the certificates only after the last package is received, each package does not need to be multiple of 4.
- <password>: string type, password for private key.

### Example

- Store CA certificate:

```
AT^SSLMNG=1,1,0,"ca-
cert2.pem",1,7,"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUVuakND
QTRhZ0F3SUJBZ0lKQU9uUXAxOTVKZIE4TUEwR0NTcUdTSWIzRFFFQkJRV
UFNSUdRTVFzd0NRWUQKVIFRR0V3SIZVekVRTUE0R0ExVUVDQk1IVFc5dW
RHRnVZEVRTUE0R0ExVUVCeE1IUW05NlpXMXWhiakVSTUE4RwpBMVVFQ
2hNSVUyRjNkRzl2ZEdneEV6QVJCZ05WQkFzVENrTnZibk4xYkhScGJtY3hGak
FVQmdOVkJBTvREWQzCmR5NTVZWE56Ykm1amlyMHhIVEFiQmdrcWhra
Uc5dzBCQ1FFV0RtbHVabTIBZVdGemMyd3VZMjI0TUI0WERURXgKTVRBeU5
ERTRNVGd4TIZvWERURTBNRGN5TURFNE1UZ3hOVm93Z1pBeEN6QUpCZ
05WQkFZVEFsVIRNUkF3RGdZRApWUVFJRXdkTmlyNTBZVzVoTVJBd0RnW
URWUVFIRXdkQ2IzcGxiV0Z1TVJFd0R3WURWUVFLRXdoVFIYZDBiMjkwCmF
ERVRNQkVHQTFVRUN4TUtRMjI1YzNWc2RHbHVaeKVTUJRR0ExVUVBeE1
OZDNkM0xubGhjM05zTG1OdmJURWQKTUJzR0NTcUdTSWIzRFFFskFSWU9
hVzVtYjBCNVIYTnpiQzVqYjlwd2dnRWINQTBHQ1NxR1NJYjNEUUVCQVFVQQ
pBNEICRHdBd2dnRUtBb0lCQVFDL0RNb3RGTEllaEVKYnpUZ2ZTdkpOZFJEe
HRqV2YzOHA5QTVqVHJONERadTRxCjhkaXdmVzRIVkFzUW1DRk5nTXNTS
U9mTVQ5NUZmY2x5ZHpmcXlwQzdhVklRQXkrbzg1WEY4WXRpVmhdloyK2s
KRUUVHvnJRcWI0NhBc05Kd2RsQXdXNmpvQ0N4ODdhZWllbzA0S1J5c3grM3I
mSl3bFIKOVNWdzR6WGNsNzcyQQpkVk9VUEQzS1kxdWZGYlhUSFJNdkdk
R"
OK
```

```
AT^SSLMNG=1,1,0,"ca-
cert2.pem",2,7,"TgyM1k2ekxoOXIIWEMxOXBBYjlnaDNITWJRaTFUbIA0YS9IMn
JlalkvCm1ONkVmQVZuem1vVU9JZXA4WXkxYU10b2YzRWdLL1dnWS9WV0w
2TW0wcmR2c1ZvWDF6aVpDUDZUV0cvK3d4TkoKQ0JZTHAwMW5BRkl4Wnl
OT21PMVJSUji1Qk5rTDdOZ29zMHU5N1RaNUFnTUJBQUdqZ2Znd2dmVXdIU
VIEVIlwTwpCQlIFRkNIT1p4RjB3eVlkUCswelk3T2syQjb3NWVqvK1JSEZCZ05W
SFNNRWdiMHdnYnFBRkNIT1p4RjB3eVlkCIArMHpZN09rMklwdzVlaIzvWUdXc
EIHVE1JR1FNUXN3Q1FZRFZRUUdFd0pWVXpFUU1BNEdBMVVFQ0JNSFRX
OXUKZEEdGdViURVFNQTRHQTFRUJ4TUhRbTk2WlcxaGJqRVJNQThHQTFV
RUNoTUIVMkYzZEc5dmRHZ3hFekFSQmdOVgpCQXNUQ2tOdmJuTjFiSFJwY
m1jeEZqQVVCZ05WQkFNVERYZDNkeTU1WVhOemJDNWpiMjB4SFRBYkJna
3Foa2IHCjl3MEJDUUVXRG1sdVptOUFIV0Z6YzJ3dVkyOXRnZ2tBNmRDblgza2
```



```
w5RHd3REFZRFZSMFRCQVV3QXdFQi96QU4KQmdrcWhraUc5dzBCQVFVRk
FBT0NBUUVBWDRZVTIGR0x2S1ZPTU5wZXJKcjRiTmttUzVQNTR4eUpiNTd1c
zUxMwpQb2tnZHFQbTZJWVZJZHzeptTdJMDfKQ2Y4OEEdraDVKYytkSC9NQyt
PQTd5elBBd3lvNUJmR3BBZX1M3puGNIckFxbDIKMlpqTDY4WTE2d1ltSXIE
anpqekM2dzJSFg3eW5ZVFVGc0NqM08vNDZEEdWcxSWxWTRtenB5OUwzb
XIKRzJDNGt2RUR3Uhc3Q05uQXJkVnIDQ1dBWMzY242ZURZZ2RINEFkTV
N3Y3dCS21ISEZWL0J4TFF5MEpkeTg5bQpBu9YN3ZrUF"
```

OK

```
AT^SSLMNG=1,1,0,"ca-
cert2.pem",3,7,"IMZmJiMmpsVGtGaWJ0TnZZRTIMSjk3UEdBZnhFMTNMUDZrb
FJOcFNYTWdFNFZZUzITcVFUdEhpCnJ3RzFJNkhzTWRwN1kybkV1UFBuenF
FOXdOdHQ4N0xaUnNpZnc3aHdXaDkveWc9PQotLS0tLUVORCBDRVJUSUZJ
Q0FURS0tLS0tCkNlcRpZmljYXRIOgogICAgRGF0YToKICAgICAgICAgICAg
W9uOiAzICgweDlpCiAgICAgICAgU2VyaWFsiE51bWJlcoKICAgICAgICAgICAg
ZTk6ZDA6YTc6NWY6Nzk6MjU6ZjQ6M2MKICAgICAgICBTaWduYXR1cmUgQ
Wxnb3JpdGhtOIBzaGExV2l0aFJTQUVuY3J5cHRpb24KICAgICAgICBJc3N1ZXi
6IEM9VVMsIFNUPU1vbnRhbmEsIEw9Qm96ZW1hbiwgTz1TYXd0b290aCwgT1
U9Q29uc3VsdGluZywgQ049d3d3LnIhc3NsLmNvbS9lbWFpbEFkZHJlc3M9aW5
mb0B5YXNzbC5jb20KICAgICAgICBWWYxpZGI0eQogICAgICAgICAgICBo3Q
gQmVmb3JIOiBPY3QgMjQgMTg6MTg6MTUgMjAxMSBHTVQKICAgICAgICAg
CAgTm90IEFmdGVyIDogSnVsIDlwIDE4OjE4OjE1IDlwMTQgR01UCiAgICAgIC
AgU3ViamVjdDogQz1VUywgU1Q9TW9udGFuYSwgTD1Cb3plbWFuLCBPPVN
hd3Rvb3RoLCBPVT1Db25zdWx0aW5nLCBDTj13d3cueWFzc2wuY29tL2VtYWi
sQWRkcmVcz1pbmZvQHlh3NsLmNvbQogICAgICAgICBQdWJsaWMgS2V5IEFsZ29yaXRobTogcn
NhRW5jcnlwGlvbogogICAgICAgICBSU0EgUHVibGljEtleTogKDIwNDggYm
I0KQogICAgICAg!"
```

OK

```
AT^SSLMNG=1,1,0,"ca-
cert2.pem",4,7,"CAgICAgICAgTW9kdWx1cyAoMjA0OCBiaXQpOgogICAgICAgI
CAgICAgICAgICAgIDAwOmJmOjBjOmNhOjKoje0OmllyOjFIOjg0OjQyOjViOm
NkOjM4OjFmOjRhOgogICAgICAgICAgICAgICAgICAgIGYyOjRkOjc1OjEwOmY
xOml2OjM1OjImOmRmOmNhOjdkOjAzOjk4OmQzOmFjOgogICAgICAgICAgIC
AgICAgICAgIGRIOjAzOjY2OmVIOjJhOmYxOmQ4OmlwOjdkOjZIOjA3OjU0OjBi
OjEwOjk4OgogICAgICAgICAgICAgICAgIDlxOjRkOjgwOmNiOjEyOjIwOmU
3OmNjOjRmOmRIOjQ1OjdkOmM5OjcyOjc3OgogICAgICAgICAgICAgICAgICAg
DMyOmVhOmNhOjkwOmJiOjY5OjUyOjEwOjAzOjJmOmE4OmYzOjk1OmM1O
mYxOgogICAgICAgICAgICAgICAgIDhiOjYyOjU2OjFiOmVmOjY3OjZmOm
E0OjEwOjQxOjk1OmFkOjBhOjliOmUzOgogICAgICAgICAgICAgICAgICAgIGE1
OmMwOmlwOmQyOjcwOjc2OjUwOjMwOjViOmE4OmU4OjA4OjJjOjdlOmVko
oglICAgICAgICAgICAgICAgICAgICAgIGE3OmEyOjdhOjhkOjM4OjI5OjFjOmFjOmM3
OmVkoMYYOjdlOjk1OmIwOjk1OgogICAgICAgICAgICAgICAgIDgyOjdkOjQ
5OjVjOjM4OmNkOjc3OjI1OmVmOmJkOjgwOjc1OjUzOjk0OjNjOgogICAgICAgIC
AgICAgICAgICAgIDNkOmNhOjYzOjViOjImOjE1OmI1OmQzOjFkOjEzOjJmOjE5
OmQxOjNjOmRiOgogICAgICAgICAgICAgICAgICAgIDc2OjNhOmNjOmI4OjdkO
mM5OmU1OmMyOmQ3OmRhOjQwOjZmOmQ4OjlxOmRjOgogICAgICAgICAgICAg
CAg"
```

OK

```
AT^SSLMNG=1,1,0,"ca-
cert2.pem",5,7,"ICAgICAgIDczOjFjOjQyOjJkOjUzOjIjOmZlOjFhOmZjOj
dkOmFiOjdhOjM2OjNmOjk4OgogICAgICAgICAgICAgICAgICAgIGRIOjg0Oj
djOjA1OjY3OmNIOjZhOjE0OjM4Ojg3OmE5OmYxOjhjOmI1OjY4OgogICAgICAgICAgIC
AgICAgICAgIGNiOjY4OjdmOjcxOjIwOjJiOmY1OmEwOjYzOmY1OjU2OjJmOmEzOjI2
```



OmQyOgogICAgICAgICAgICAgICAgIGI3OjZmOmIxOjVhOjE3OmQ3OjM4  
Ojk5OjA4OmZlOjkzOjU4OjZmOmZlOmMzOgogICAgICAgICAgICAgID  
EZoQj5OjA4OjE2OjBiOmE3OjRkOjY3OjAwOjUyOjMxOjY3OjlzOjRIOjk4OgogIC  
AgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIDM2Ojc5CiAgIC  
AgICAgICAgICAgICBFeHBvbmVudDogNjU1MzcgKDB4MTAwMDEpCiAgICAgIC  
AgWDUwOXYzIGV4dGVuc2lvbnM6CiAgICAgICAgICAgIFg1MDI2MyBTdWJqZ  
WN0IEtLeSBJZGVudGlmaWVyoAiKICAgICAgICAgICAgIDl3OjhFOjY3OjEx  
Ojc0OkMzOjI2OjFEOjNGOkVEOjMzOjYzOkIzOkE0OkQ4OjFEOjMwOkU1OkU4  
OkQ1CiAgICAgICAgICAgICAgIFg1MDI2MyBBdXRob3JpdHkgS2V5IElkZW50aWZpZ  
XI6IAogICAgICAgICAgICAgICAg2V5aWQ6Mjc6OEU6Njc6MTE6NzQ6QzM6Mj  
Y6MUQ6M0Y6RUQ6MzM6NjM6QjM6QTQ6RDg6MUQ6MzA6RTU6RTg6RDUK  
ICAgICAgICAgICAgICAgIERpk5hbWU6L0M9VVMvU1Q9TW9udGFuYS9"

OK

AT^SSLMNG=1,1,0,"ca-  
cert2.pem",6,7,"MPUJvemVtYW4vTz1TYXd0b290aC9PVT1Db25zdWx0aW5nL  
0NOPXd3dy55YXNzbC5jb20vZW1haWxBZGRyZXNzPWluZm9AeWFzc2wuY29  
tCiAgICAgICAgICAgICAgICBzZXJpYWw6RTk6RDA6QTc6NUY6Nzk6MjU6RjQ6  
M0MKCiAgICAgICAgICAgICAgIg1MDI2MyBCYXNpYyBDb25zdHJhaW50czogCiAgI  
CAgICAgICAgICAgICBDQTpUUIVFciAgICBTaWduYXR1cmUgQWxnb3JpdGht  
OiBzaGExV2l0aFJTQUVuY3J5cHRpb24KICAgICAgICA1Zjo4NjoxNDpmND01M  
To4YjpiYzphNT0ZTozMDpkYT01ZTphYzo5YTpmODo2YzpkOToyNjoKICAgICAgI  
gICA0Yj05MzpmOTplMzoxYzo4OT02Zj05ZTp1ZTp1Mzo5ZDo3NzozZTo4OToyM  
Do3NjphMzplNjoKICAgICAgICBIODo4NjoxNToyMTpkYjplMj0zMzpiMj0zNDpkNT  
pkMDo5ZjpmMzp1MTphND04Nzo5Mj01YzoKICAgICAgICBmOTpkMTpmZj0zMD  
oyZj04ZTowMzpiYzpiMzozYzowYzozMjphMzo5MDo1ZjoxYT05MDoxZToKICAgI  
CAgICBhZj05ZDpmMzo5ZTp1NzowNzowMjphOTo3ZDoyNzo2Njo2MzoyZjphZj0  
xODpkNzphYzoxODoKICAgICAgICA5ODo4Yz04Mzo4Zj0zODpmMzowYjphYz0  
zNjoxMDo3NTpmYjpjYTo3NjoxMzo1MDo1YjowMjoKICAgICAgICA4Zj03MzpiZjpl  
MzphMDplZTo4Mzo1MjoyNT01NDpjZToyNjpjZTo5YzpiZDoyZj03OTphYjoKICAgI  
CAgICAxYj02MDpiODo5MjpmMTowMzp1MDpmYzozYjowODpkOTpjMDphZDpk  
NT03MjowODoyNT04MDoKICAgICAgICA2MToyZDpkYz05ZjphNzo4Mz"

OK

AT^SSLMNG=1,1,0,"ca-cert2.pem",7,7,"o2MjowNzo0NzplMDowNzo0Yzo0YjowNzozMDo...  
zoKICAgICAgICAxYzo1NTo3ZjowNzoMjp...  
oxYToxNzplZTp...  
o2Mj...  
To2Mj...  
MToxMzo1ZDpjYj...  
KICAgICAgICBmNT...  
MTpkY...  
DpkY...  
Zjo3ZpjYQo="

OK

- Store client certificate:

AT^SSLMNG=1,0,0,"client-cert.pem",1,7,"Q2VydGlmaWNhdGU6CiAgICBEYXRhOgogICAjCAgIFZlcNpb246IDMgKDB4MikKICAgICAjICBTZXJpYWwgTnVtYmVyOgogICAjCAgICAgICAgICAjCAgICAjCA4Nzo0YT03NTpiZTo5MTo2NjpkODozZAooglCAgICAgIFNpZ25hdHVyZSBBbGdvcmloA0G06lHN0YTFxaXRoUINBRW5jcnIwdGlvbogICAjCAgIElzc3VlcjogQz1VUywgU1Q9T3JZ29uLCBMPVBvcnRsYW5kLCBPPXlhU1NMLCBPVT1Qcm9ncmFtbWluZywgQ049d3d3LnIhc3NsLmNvbS9lbWFpbEFkZHJlc3M9aW5mb0B5YXNzbC5jb20KICAgICAjICAjCBWYWyxpZGI0eQoqlCAgICAjCAgICAjCBOb3QqQmVm



b3JlOjBPY3QgMjQgMTg6MjE6NTUgMjAxMSBHTVQKICAgICAgICAgICAgTm9  
0IEFmdGVyIDogSnVsIDlwDE4OjlxOjU1IDlwMTQgR01UCiAgICAgICAgU3Viam  
VjdDogQz1VUywgU1Q9T3JZ29uLCMPVBvcnRsYW5kLCBPPXlhU1NMLCBP  
VT1Qcm9ncmFtbWluZywgQ049d3d3LnIhc3NsLmNvbS9lbWFpbEFkJZHJc3M9a  
W5mb0B5YXNzbC5jb20KICAgICAgICBTdWJqZWN0IFB1YmxpYyBLZXkgSW5  
mbzoKICAgICAgICAgICAgUHVibGjlEtleSBBbGdvcmloaG06IHJzYUVuY3J5cH  
RpB24KICAgICAgICAgICAgUINBIFB1YmxpYyBLZXk6ICgyMDQ4IGJpdCkKICA  
gICAgICAgICAgICAgIE1vZHVsdxMgKDIwNDggYml0KToKICAgICAgICAgICAgI  
CAgICAgICAwMDpjMzowMzpkMToyYjmpzTozOTphNDozMjo0NTozYjo1MzpjO  
Do4NDoyYjoKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgI  
yYTo"

OK

OK

OK

AT^SSLMNG=1,0,0,"client-cert.pem",4,7,"CAgWDUwOXYzIEJhc2ljLENvbnN0cmFpbnRzOiAKICAgICAglCAgICAglCAgIENBOIRSVUUKICAgIFNpZ25hdHVyZSBBbGdvcmloAaG06lHNoYTF



```
XaXRoUINBRW5jcnIwdGlvgogICAgICAgIDFjOjdjOjQyOjgxOjI5OjIIoJlxOmNmO
mQwOmQ4OmMxOjU0OjZmOmNjOmFIOjE0OjA5OjM4OgogICAgICAgIGZmOj
Y4Ojk4OjhOjk1OjUzOjc2OjE4OjdiOmU2OjMwOjc2OmVjOjI4OjBkOjc1OmE3O
mRIOgogICAgICAgIGUwOmNkOjh1OmQ1OjU1OjIzOjZhOjQ3OjJiOjRIOjhkOmZj
OjdkOjA2OmEzOmQ4OjBmOmFkOgogICAgICAgIDVIOmQ2OjA0OmM5OjAwOj
MzOmZiOjc3OjI3OmQzOmI1OjAzOmIzOjdiOjlxOjc0OjMxOjBiOgogICAgICAgID
RhOmFmOjJkOjFhOmIzOjkzOjh1OmNjOmYzOjVmOjNkOjkwOjNmOmNjOmUzO
jU1OjE5OjkxOgogICAgICAgIDdiOjc4OjI0OjJiOjRhOjA5OmJiOjE4OjRIOjYxOjJk
OjjOmM2OjBhOmEwOjM0OjkxOjg4OgogICAgICAgIDcwOjZiOjNiOjQ4OjQ3Om
JjOjc5Ojk0OmEyOmEwOjRkOjMyOjQ3OjU0OmMyOmEzOmRjOjJiOgogICAgIC
AgIGQyOjUxOjRjOjI5OjM5OjExOmZmOmUyOjE1OjVIOjU4Ojk3OjM2OmY2Om
U5OjA2OjA2Ojg2OgogICAgICAgIDBIOjhkOjk1OjAzOjcyOmlyOjhiOjE5OjdjO
mU5OjE0OjZlOmExOjg4OjczOjY4OjU4OgogICAgICAgIDZkOjcxOjVIOmMyOm
Q1OmQzOjEzOmQyOjVmOmRIOmVhOjAzOmJlOmUyOjAwOjQwOmU1OmNIO
gogICAgICAgIGZkOmU2OjkyOjMxOjU3OmMzOmViOmJiOjY2OmFj"
```

OK

```
AT^SSLMNG=1,0,0,"client-
cert.pem",5,7,"OmNiOjJmOjFhOmZhOmUwOjYyOmEyOjQ3OgogICAgICAgIGY
0OjkzOjQzOjJhOjRiOjZjOjVIOjBhOjJmOmY5OmU3OmU2OjRhOjYzOjg2OmlwO
mFjOjJhOgogICAgICAgIGExOmViOmI0OjViOjY3OmNkOjMyOmU0OmI2OjExOj
RIOjIhOjcyOjY2OjBkOmEyOjRhOjc2OgogICAgICAgIDhmOmZlOjlyOmJjOjgzOm
ZkOmRiOml3OmQ1OmE5OmVIOjA1OmM5OmIxOjcxOjdlOjFiOjJiOgogICAgICA
gIGUxOmUzOmFmOmMwCi0tLS0tQkVHSU4gQ0VSVEIGSUNBVEUtLS0tLQpN
SUIFbURDQ0E0Q2dBd0ICQWdJSkFJZEtkYjZSwnRnOU1BMEdDU3FHU0liM0
RRRUJCUVVBTDIHT01Rc3dDUVIECIZRUUdFd0pWVXpFUE1BMEdBMVVFQ0
JNR1QzSmxaMj1TVJFd0R3WURWUVFIRXdoUWIzSjBiR0Z1WkRFT01Bd0cK
QTFVRUNoTUZIV0ZUVTB3eZEQVNCZ05WQkFzVEMxQnliMmR5WVcxGFX
NW5NUII3RkFZRFZRUURFdzEzZDNjdQpIV0Z6YzJ3dVkyOXRNujB3R3dZSkv
WklodmNOQVFrQkZnNXBibVp2UUhsaGMzTnNbU52YIRBZUZ3MhHNEV3C
k1qUXhPREI4TIRWYUZ3MhHOREEZTwpBeE9ESXhOVFZhTUIHT01Rc3dDUV
IEVIFRR0V3SIZVekVQTUEwR0ExVUUKQ0JNR1QzSmxaMj1TVJFd0R3WUR
WUVFIRXdoUWIzSjBiR0Z1WkRFT01Bd0dBMVVFQ2hNRmVXRIRVMHd4RkR
BUwpCZ05WQkFzVEMxQnliMmR5WVcxGFXNW5NUII3RkFZRFZRUURFdzE
zzDNjdWVXRnpjMnd1WTI5dE1SMHdHd1IKCktvWklodmNOQVFrQkZnNXBibV
p2UUhsaGMzTnNbU52YIRDQ0FTSXdEUVIKS29aSWh"
```

OK

```
AT^SSLMNG=1,0,0,"client-
cert.pem",6,7,"2Y05BUUVCQIFBRGdnRVAKQURDQ0FRb0NnZ0VCQU1NRDB
TditPYVF5UIR0VHIJUXJLbngwbXlycUtsSUhSOWFtTnJJSE1vN1F1bWw3eHN
ORQpudFNCU1AwdGFLS0xaN3VoZGNnMkxFcINHL2VMdXM4TitIL3M4WUVIZ
TVzRFI1cS9aY3gvWINSchB1Z1VpVnZrCk5QzKzQINUVDkN09ucDQ0UUZX
VnBHbUUwS04wanhBbkV6djBZYmZOMUViREtFNzImR2pTalhrNGM2VzN4dCs
KdjA2WDBCRCG9xQWd3Z2E4Z0MwTVV4WFJudERLQ2I0Mkd3b2hBbVRhRHV
oNUFjaUIYMTFKbEpIT3d6dTThaemE3LwpIR3g3d0JRRDFFXIEVkj0TzZNN281
bGVuY2paREIXejZclpWQ2JiYmZxc3UvOGxUTVRSZWZSeDA0WkFHQk93Clk
3VnlUakRFbDRTR0xWWXYxeFgzJhDdTlmeGI1ZnVodXRNQ0F3RUFBYU9CO
WpDQjh6QWRCZ05WSFE0RUZnUVUKTTl0Rp0ZG9oeGgrVkJbWVRBbFZUTVE4d0R
VGWmNb2djTUDBMVvkSXdtQnV6Q0J1SUFVTTl0Rp0ZG9oeGgrVkJbWVRBbFZUTVE4d0R
NUhISnRIRlpjQ2hnWINrZ1pFd2dZNHhDekFKQmdOVkJBWVRBbFZUTVE4d0R
RWURWUVFJRXdaUGNtVm5iMjR4CkVUQVBCZ05WQkFjVENGQnZjblJzWVc
1a01RNhdEQVIEVIFRS0V3VjVZV5kUVERFVU1CSUdBMVVFQ3hNTFVISnYK
WjNKaGJXMXBibWN4RmpBVUJnTlZCQU1URFhkM2R5NTVZWE56YkM1amly
MHhIVEFiQmdrcWhraUc5dzBCQ1FFVwpEbWx1Wm05QWVXRnpjMnd1WTI5d
```



Gdna0FoMHAxdnBGbTJEMHdEQVIEVIIwVEJBVXdBd0VCL3pBTkJna3Foa2IH  
CjI3MEJBUVVGQUFPQ0FRRUFISHhDZ1NtZUljl1EyTUZVYjh5dU"

OK

AT^SSLMNG=1,0,0,"client-cert.pem",7,7,"ZBazQvMmlZbXBWVGRoAc1aklyN0NnTmRhZmUKNE0yTzFW  
VWpha2NyVG8zOGZRYWoyQSt0WHRZRXIRQXorM2NuMDdVRHMzc2hkREV  
MU3E4dEdyT1Rqc3p6WHoyUQpQOHpqVIJtUmUzZ2tMa29KdXhoT1ITMmN4Z  
3FnTkpHSWNHczdTRWU4ZVpTaW9FMHISMVRDbzl3dTBSRk1LVGtSci8rSVZ  
YbGIYTnZicEJnYUdEbzbJkbFFOeXNvc1pmT2tVYnFHSWMyaFiWEZld3RYVEU  
5SmYzdW9EdnVJQVFPE8KL2VhU01WZkQ2N3Rtck1zdkd2cmdZcUpIOUpO  
REtrdHNYZ292K2VmbVNtT0dzS3dx2b2V1MFcyZk5NdVMyRVV1YQpjvVIOb2tw  
MmovNGI2SVA5MjdmVnFINEZ5YkZ4ZmhzcjRIT3Z3QT09Ci0tLS0tRU5EIENFUI  
RJRkIDQVRFLS0tLS0K"

OK

- Store Client-Key certificate:

AT^SSLMNG=1,2,0,"client-key.pem",1,3,"LS0tLS1CRUdTjIBSU0EgUFJJVkJURSBRLVktLS0tLQpNSUIFcE  
FJQkFBS0NBUVBd3dQUksvNDVwREpGTzFQSWhDc3FmSFNhdmdFvcVVnZ  
EgxcVkyC2djeWp0QzZhWHZHChncwU2UxSUZJL1Mxb29vdG51NkYxeURZc1N0  
SWi5NHU2enczNTcrenhnUjU3bXdOSG1yOWx6SDIsSkdtbTZCU0oKVytRMDk4  
V3dGSIAxWjNzNmVuamhBVlpXa2FZVFFvM1NQRUNjVE8vUmh0ODNVUnNNb  
1R2MThhTktOZVRoenBiZgpHMzYvVHBmUUVPaW9DRENCCnlBTFF4VEZkr2  
UwTW9KdmpZYkNpRUNaTm9PNkhrQnJaGZYVW1Va2M3RE83eG5OCnJ2OT  
RiSHZBRWdQVVRuSU5VRzA3b3p1am1WNmR5TmtNaGJQWml0bFVKdHR0K  
3F5Ny95Vk14TkY1OUhIVGhrQVkJRTdCanRYSk9NTVNYaElZdFZpL1hGZmQv  
d0s3MS9GdmwrNkc2MHdJREFRQUJBb0ICQVFDaTV0aGZFSEZrQ0o0dQpiZE  
Z0SG9YU0NyR01SODRzVvxZ0VwNVQzcEZNSFczcVdYdnkNnJaeHRtS3E5  
amhGdVJqSnYrMWJCTIp1T09sCnISvhMZ3ImYitWWIAzWnZTYkVSd2xvdUZp  
a04zcmVPM0VEVm91N2dlcUgwdnBmYmhtT1dGTTJZQ1dBdE1IYWMKUE0zb  
WIPNUhrbmtMV2dEaVhsOFJmSDM1Q0xjZ0Jva3FYzJBBcXIMaDhMTzhKS2xIS  
mc0ZkFDMytJWnBUVzIzVApLNnVVZ21oRE50ajMOFlpL0xWQlhRMHpZT3FrZ  
lg3b1MxV1JWdE5jVjQ4ZmxCY3ZxdDdwbnFqMHo0cE1qcURrCIzuT3l6MCtHeF  
drOdh5UWdpMXIXRFBwckVqdWFaOEhmeHBheXBkV1NEWnNKUW1na0VFW  
FVVT1FYT1VqUU5ZdVUKYIJIZWo4cFpBb0dCQU9va3AvbHB"

OK

AT^SSLMNG=1,2,0,"client-key.pem",2,3,"NK2x4M0ZKOWIDRW9MMG5IdW5JVzzjeEhlb2dObEZIRVdCWT  
ZnYkEvb3MrbQpiQjZ3QmlrQWorZDNkcxpieXNmWlhwcy9KcEJTcnZ3NGtBQVV  
1N1FQV0pUbkwycCtIRTCSWRReFdSOU9paHFOCnAxZHNJdGpsOUG0eXBo  
RExaS1ZWQTRlbuP3V013OWUySjdKTnVqRGFSNDIVMHoyTGHJMIVtRmlsQ  
W9HQkFOVTQKRzhPUHhaTU1Sd3R2TIpMRnNJMUd5SkIzai9XQUN2ZnZvZjZ  
BdWJVcXVzb1lzRjJsQjIDVGpkaWNCQnpVWW82bQpKb0VCLzg2S0ttTTBOVU  
NxYIIEZWITTnFWMDJYnEyVFRsYVFDMjKjYzRzTXJpYzkzazd3cXNWc2VHZH  
NsRktjCk4yZHNMZSs3cjkrbWtEekVSO CtObHA2WXfIU2Z4YVpRM0xQdyszUV  
hBb0dBWG9NSllyMjZmS0svUW5UMWZCeIMKYWNrRURZVitQajBrRXNNWW  
UvTXA4MThPZG14WmRIukJoR21kTXZQTklxdXdOYnBLc2p6bDJWaTJZazIkM  
3VXZQpDc3BUc2l6M25yTnJDbHQ1WmV4dWtVNINJUGI4L0JidDAzWU00dXgv  
c21rVGEzz09Xa1prdEY2M0phQmFkVHBMCjc4YzhQdmY5SnJnZ3hKa0ttbk8rd  
3hrQ2dZRUF1a1NURkt3MEDudGZrV0NzOTdUV2dRVTJVk05NkdYY3J5N2M  
KWVQ3SmZiaC9oL0E3bXdpQ0tUzk9jazRSMWJIQkRBZWdtWkZLalgvc2VjL3h  
PYIhwGV4aTk5cDI2R1JOSWp3Two4dFpSOVlmWW1jQVJJRjBQS2YxYjRxN1  
pITmtovm0zOGhOQmY3UkFWSEJnaDU4UTITOWZRbm1xVnp5TEpBM3VICjQ



yQULvQzhDZ1IBUjBFdlBHMmU1bnhCMVI0WmxyakhDeGpDc1dRWIEyUSsxY0  
FiMzhOUEIZbnlvMm03MkIUL1QKZjEvcWIxcy"

OK

AT^SSLMNG=1,2,0,"client-  
key.pem",3,3,"8yU3BIODFIU3dqQTM0eTJqZFEwZVRTRTAxVmR3WEltL2N1eE  
tibWpWeIJoME0wNk1Pa1dQNXBaQQo2MIA1R1IZNIVkMkpTN0R6K1o5ZEtkVT  
R2aldyeWx6bmsxTTBvVVZkRXpsbFFrYWhuODMxdnc9PQotLS0tLUVORCBSU  
0EgUFJJVkJURSBLRVktLS0tLQo="

OK



# 4 Work with SSL

## 4.1 Open a Secure Socket

As per AT command requirement, we provides an AT command for opening a normal socket or a secure socket. In case of normal socket creation, this AT command will simply use the Real Time Executive (REX) socket interface to create and open the common TCP socket. For secure socket creation, this AT command will use both socket interface and CyaSSL library for creation of socket.

CyaSSL Socket Open uses the AT Command AT^SSLO:

**AT^SSLO=<SSL\_id>,<remote\_IP>,<remote\_port>,[<mode>,<TimeOut>]**

Where:

- <SSL\_id>: SSL socket ID.
  - 1: Secure socket connection
  - 0: Normal socket connection
- <remote\_IP>: string type; IP address, IP or hostname of the server.
- <remote\_port>: port, the value ranges from 1 to 65535; remote port of the server (usually 443).
- <mode>: async mode (optional, it will take the value as 0 by default).
  - 0: Sync mode
  - 1: Async mode
    - For Sync mode, data will be received in synchronous mode. If run AT^SSLRX command, then it will receive the data from server.
    - For Async mode, data will be received in asynchronous mode (i.e.) whenever data is available in the server, it will be received automatically.
- <TimeOut>: timeout value in seconds (60–180 seconds). It is optional parameter. It will take the value as 90 seconds by default.

### Example

CyaSSL secure socket open:

- Sync mode:

AT^SSLO=1,"192.166.63.155",443,0,60

OK



- Async mode:  
AT^SSLO=1,"192.166.63.41",473,1,60  
OK

^SSLRX: 767

## 4.2 Socket Connection Status

An AT command is provided to know the current connection state of the socket based on the <SSL\_id>.

If the request is for normal socket ID, it will return connection closed or connection opened if normal socket is available, or else it will return connection not opened.

If the request is for secure socket ID, it will return connection opened or connection closed if secure socket is available, or else it will return connection not opened.

CyaSSL connection status can be obtained using the AT command AT^SSLSTAT.

This command queries the status of a secure or normal socket.

AT^SSI STAT=<SSI\_id>

Where:

- <SSL\_id>: SSL socket ID.
    - 1: secure socket connection
    - 0: normal socket connection
  - <conn\_state>: values are as follows:
    - 1: normal connection opened
    - 2: normal connection not opened
    - 3: secure connection opened
    - 4: secure connection not opened



### Example

When the socket connection is established:

AT^SSLSTAT=1

^SSLSTAT: Secure connection opened

OK

## 4.3 Exchange Data Through a Secure Socket

### 4.3.1 Transmit Data

Once the socket connection is established, an AT Command is provided to write data into the opened socket.

Data can be transmitted through secure socket using the AT command AT^SSLTX.

**AT^SSLTX=<SSL\_id>,<data\_buffer>[,<TimeOut>]**

Where:

- <SSL\_id>: SSL socket ID.
  - 1: secure socket connection
  - 0: normal socket connection
- <data\_buffer>: string type, the data which are needed to transmit [1-1024 bytes].
  - If the <encode\_ok> is set to 1, then the input buffer should be 768 bytes of raw data.
  - If the <encode\_ok> is set to 0, then the input buffer should be 1024 bytes of raw data.
  - If <encode\_ok> in AT^SSLEN command is 1, then it should be Base 64 encoded format data. Otherwise it should be normal plain data.
- <TimeOut>: maximum blocking timeout in seconds. It is an optional parameter. It can be omitted, and in this case the default timeout configurable with AT^SSLCFG will be used for secure socket TX and for normal socket TX, the default timeout value (60s) will be used.

### Example

(If <encode\_ok> is 1 for AT^SSLEN command):

AT^SSLTX=1,"SGVsbG8=",60

OK

### 4.3.2 Receive Data

An AT command is provided to read data from the socket.

Data can be read from the socket using the AT command AT^SSLRX.

**AT^SSLRX=<SSL\_id>,<Maxlength>[,<TimeOut>]**



Where:

- <SSL\_id>: SSL socket ID.  
1: secure socket connection  
0: normal socket connection  
In case of normal socket connection, effect and process will be the same as TCP.
- <Maxlength>: specifies the maximum number of bytes that will be read from the socket.
- <TimeOut>: specifies the maximum blocking timeout. It can be omitted, and in this case the default timeout configurable with AT^SSLCFG will be used for secure socket RX and for normal socket RX the default Timeout value (60 seconds) will be used.
- <LengthOfRec>: the actual number of bytes received.
- <Received\_data>: the received data.  
If <encode\_ok> in AT^SSLEN command is 1, then it is Base 64 encoded format data (the length of the <Received\_data> is differ from <LengthOfRec>, because the <Received\_data> is in Base 64 encoded format). Otherwise, the actual plain data will be displayed.

#### Example

(If <encode\_ok> is 1 for AT^SSLEN command):

AT^SSLRX=1,5,60

^SSLRX: 5

SGVsbG8=

OK

## 4.4 Close Socket

At any time, users may want to close the socket for closing the connection.

Socket closure is accomplished by AT command AT^SSLC:

**AT^SSLC=<SSL\_id>**

Where:

- <SSL\_id>: SSL socket ID.  
1: Secure socket connection  
0: Normal socket connection

#### Example

Close CyaSSL secure socket:

AT^SSLC=1

OK



# 5 SSL AT Commands

In order to meet the requirements of AT commands for SSL, an Interface layer called CyaSSL Service Layer is designed to run as a separate task that makes use of both CyaSSL Library services and TCP for establishing normal or secure connection based on the request from AT commands.

The following AT commands are designed to meet the requirements of SSL.

No.	Requirement	Description
1	AT^SSLEN=<SSL_id>,<Enable>[,<encode_ok>]	Enable or disable a secure or normal socket.
2	AT^SSLCFG=<SSL_id>,<TimeOut>[,<cipher_suite>,<scur_level>]	Configure the properties of secure socket.
3	AT^SSLSTAT=<SSL_id>	Query the status of a secure or normal socket.
4	AT^SSLO=<SSL_id>,<remote_IP>,<remote_port>[,<mode>,<TimeOut>]	Create and open a secure or normal socket.
5	AT^SSLTX=<SSL_id>,<data_buffer>[,<TimeOut>]	Send data through the secure or normal socket.
6	AT^SSLRX=<SSL_id>,<Maxlength>[,<TimeOut>]	Receive the data through the secure or normal socket.
7	AT^SSLC=<SSL_id>	Close secure or normal socket.
8	AT^SSLMNG=<SSL_id>,<data_type>,<action>,<file_name>,[<package_id>,<total_no_of_packages>,<cert_info>],[<password>]	Manage certificates and other security data like private key.



# 6 SSL Error Codes

The table below lists all the error reports generated by the SSL AT commands in accordance with the selected format.

Numerical Format: AT+CMEE=1	Verbose Format: AT+CMEE=2
100	Unknown Error
2101	Operations failed due to system error
2102	Socket not enabled
2103	Socket not connected
2104	Socket already enabled
2105	Socket already connected
2107	SSL error during handshake
2109	Fail to connect specified address
2110	Invalid arguments
2111	Certification error
2112	Invalid Operation
2113	Certificate maximum limit reached
2114	Network timeout
2115	SSL read failed
2116	SSL write failed
13	SIM Failure



# 7 Abbreviations

Acronym or Abbreviation	Expansion
CA	Certification Authority
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
PDP	Packet Data Protocol
SMTP	Simple Mail Transfer Protocol
REX	Real Time Executive
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security