BC66&BC66-NA SSL Application Note

NB-IoT Module Series

Rev. BC66&BC66-NA_SSL_Application_Note_V1.0

Date: 2020-02-05

Status: Released

Our aim is to provide customers with timely and comprehensive service. For any assistance, please contact our company headquarters:

Quectel Wireless Solutions Co., Ltd.
Building 5, Shanghai Business Park Phase III (Area B), No.1016 Tianlin Road, Minhang District, Shanghai, China 200233
Tel: +86 21 5108 6236
Email: info@quectel.com

Or our local office. For more information, please visit:
http://www.quectel.com/support/sales.htm

For technical support, or to report documentation errors, please visit:
http://www.quectel.com/support/technical.htm
Or email to: support@quectel.com

GENERAL NOTES

COPYRIGHT

About the Document

Revision History

Version	Date	Author	Description
1.0	2020-02-05	Taber JIANG	Initial

Contents

Table Index

1 Introduction

This document describes how to use the SSL functionality of Quectel BC66 and BC66-NA modules. In some cases, in order to ensure communication privacy, the communication between the server and the client should be in an encrypted way to prevent data from eavesdropping, tampering, or forging during the communication process. The SSL function meets these demands.

1.1. SSL Versions

The following SSL versions are supported by BC66 and BC66-NA .

Table 1: Supported SSL Versions

SSL Version
TLS1.0
TLS1.1
TLS1.2

1.2. SSL Cipher Suites

The following table shows SSL cipher suites supported by Quectel BC66 and BC66-NA modules. Please refer to https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml for details of cipher suites.

Table 2: Supported SSL Cipher Suites (Official IANA Names)

Cipher Suite Code	Cipher Suite Name
0X003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0X0035	TLS_RSA_WITH_AES_256_CBC_SHA

0X003C	TLS_RSA_WITH_AES_128_CBC_SHA256
0X002F	TLS_RSA_WITH_AES_128_CBC_SHA
0X000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0X00AF	TLS_PSK_WITH_AES_256_CBC_SHA384
0X008D	TLS_PSK_WITH_AES_256_CBC_SHA
0X00AE	TLS_PSK_WITH_AES_128_CBC_SHA256
0X008C	TLS_PSK_WITH_AES_128_CBC_SHA
0X008B	TLS_PSK_WITH_3DES_EDE_CBC_SHA
0X00FF	TLS_EMPTY_RENEGOTIATION_INFO_SCSV

2 Description of SSL AT Commands

2.1. AT Command Syntax

Table 1: Types of AT Commands and Responses

Test Command	**AT+<cmd>=?**	This command returns the list of parameters and value ranges set by the corresponding Write Command or internal processes.
Read Command	**AT+<cmd>?**	This command returns the currently set value of the parameter or parameters.
Write Command	**AT+<cmd>=<p1>[,<p2>[,<p3>[...]]]**	This command sets the user-definable parameter values.
Execution Command	**AT+<cmd>**	This command reads non-variable parameters affected by internal processes in the UE.

NOTES

1. **<...>**: Parameter name. Angle brackets themselves do not appear in the command line.
2. **[..]**: Optional parameter of a command or an optional part of TA information response is enclosed in square brackets. Brackets themselves do not appear in the command line. When a parameter is not given, new value equals to its previous value or its default setting, unless otherwise specified.
3. **Underline**: Underlined parameter value is the default setting of parameter.

2.2. Description of AT Commands

2.2.1. AT+QSSLCFG Configure Parameters of an SSL Context

The command is used to configure optional parameters for SSL functionalities.

AT+QSSLCFG Configure Parameters of an SSL Context	
Test Command **AT+QSSLCFG=?**	Response **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of

	supported **<connectID>**s**)** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"seclevel"[,(**range of supported **<seclevel>**s**)]** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"dataformat"[,(**list of supported **<send_data_format>**s**),(**list of supported **<recv_data_format>**s**)]** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"timeout"[,(**range of supported **<timeout>**s**)]** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"debug"[,(**range of supported **<debug_level>**s**)]** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"cacert"** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"clientcert"** **+QSSLCFG: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),"clientkey"** **OK**
Write Command Query the setting of the context: **AT+QSSLCFG=<contextID>,<connectID>**	Response **+QSSLCFG: <contextID>,<connectID>,"seclevel",<seclevel>** **+QSSLCFG: <contextID>,<connectID>,"dataformat",<send_data_format>,<recv_data_format>** **+QSSLCFG: <contextID>,<connectID>,"timeout",<timeout>** **+QSSLCFG: <contextID>,<connectID>,"debug",<debug_level>** **+QSSLCFG: <contextID>,<connectID>,"cacert",<checksum>** **+QSSLCFG: <contextID>,<connectID>,"clientcert",<checksum>** **+QSSLCFG: <contextID>,<connectID>,"clientkey",<checksum>** **OK** Or **ERROR**
Write Command **AT+QSSLCFG=<contextID>,<connectID>,"seclevel"[,<seclevel>]**	Response If **<seclevel>** is omitted, query the authentication mode for the specified SSL context:

	+QSSLCFG: <contextID>,<connectID>,"seclevel",<seclevel> **OK** If **<seclevel>** is specified, configure the authentication mode for the specified SSL context: **OK** If there is any error: **ERROR**
Write Command **AT+QSSLCFG=<contextID>,<connectID>,"dataformat"[,<send_data_format>,<recv_data_format>]**	Response If **<send_data_format>** and **<recv_data_format>** are omitted, query the format of sent/received data: **+QSSLCFG: <contextID>,<connectID>,"dataformat",<send_data_format>,<recv_data_format>** **OK** If **<send_data_format>** and **<recv_data_format>** are specified, configure the format of data to be sent/received: **OK** If there is any error: **ERROR**
Write Command **AT+QSSLCFG=<contextID>,<connectID>,"timeout"[,<timeout>]**	Response If **<timeout>** is omitted, query the timeout of connection and message delivery for the specified SSL context: **+QSSLCFG: <contextID>,<connectID>,"timeout",<timeout>** **OK** If **<timeout>** is specified, configure the timeout of connection and message delivery for the specified SSL context: **OK** If there is any error: **ERROR**
Write Command **AT+QSSLCFG=<contextID>,<connectID>,"debug"[,<debug_level>]**	Response If **<debug_level>** is omitted, query the printable debug log level for the specified SSL context: **+QSSLCFG: <contextID>,<connectID>,"debug",<debug**

	_level> **OK** If **<debug_level>** is specified, configure the printable debug log level for the specified SSL context: **OK** If there is any error: **ERROR**
Write Command Configure the content of trusted CA certificate in PEM format for the specified SSL context: **AT+QSSLCFG=<contextID>,<connectID>,"cacert"**	Response **>** After the above response, input the data to be sent. Tap "CTRL+Z" to send the data and tap "ESC" to cancel the operation. **+QSSLCFG: <contextID>,<connectID>,"cacert",<checksum>** **OK** If there is any error: **ERROR**
Write Command Configure the content of client certificate in PEM format for the specified SSL context: **AT+QSSLCFG=<contextID>,<connectID>,"clientcert"**	Response **>** After the above response, input the data to be sent. Tap "CTRL+Z" to send the data and tap "ESC" to cancel the operation. **+QSSLCFG: <contextID>,<connectID>,"clientcert",<checksum>** **OK** If there is any error: **ERROR**
Write Command Configure the content of client private key in PEM format for the specified SSL context: **AT+QSSLCFG=<contextID>,<connectID>,"clientkey"**	Response **>** After the above response, input the data to be sent. Tap "CTRL+Z" to send the data and tap "ESC" to cancel the operation. **+QSSLCFG: <contextID>,<connectID>,"clientkey",<checksum>** **OK**

	If there is any error: **ERROR**
Maximum Response Time	300 ms
Characteristics	Take effect immediately. Invalid after powering down.

Parameter

<contextID>	Integer type. SSL context index. The range is 1-3.
<connectID>	Integer type. SSL connect index. The range is 0-5.
<seclevel>	Integer type. Authentication mode. 0 No authentication 1 Manage server authentication 2 Manage server and client authentication if requested by the remote server
<send_data_format>	Integer type. The format of the sent data. 0 Text format 1 Hex format
<recv_data_format>	Integer type. The format of the received data. 0 Text format 1 Hex format
<timeout>	Integer type. Timeout value of connection or message delivery. The range is 10-300. The default value is 90. Unit: second.
<debug_level>	Integer type. The printable debug log level. 0 No debug log 1 Error debug log 2 State debug log 3 Info debug log 4 Detail debug log
<checksum>	Integer type. Number of certificate bytes entered.

NOTES

1. Currently only **<contextID>**=1 is supported.
2. **<debug_level>** is used during debugging only. And the bigger the value is, the more log will be generated.
3. If **<seclevel>** is set to 0, no security data will be needed. If **<seclevel>** is set to 1, server CA certificate needs to be configured. If **<seclevel>** is set to 2, client certificate, server CA certificate and client private key need to be configured.

2.2.2. AT+QSSLOPEN Open an SSL Socket to Connect a Remote Server

This command is used to open a socket service.

AT+QSSLOPEN Open an SSL Socket to Connect a Remote Server	
Test Command **AT+QSSLOPEN=?**	Response **+QSSLOPEN: (**range of supported **<contextID>**s**),(**range of supported **<connectID>**s**),<host_name>,<port>,(**list of supported **<connect_mode>**s**)** **OK**
Read Command **AT+QSSLOPEN?**	Response **OK**
Write Command **AT+QSSLOPEN=<contextID>,<connectID>,<hostname>,<port>,<connect_mode>**	Response **OK** **+QSSLOPEN: <contextID>,<connectID>,<err>** If there is any error: **ERROR**
Maximum Response Time	**<timeout>** of **AT+QSSLCFG** (default 90s), determined by network
Characteristics	/

Parameter

<contextID>	Integer type. SSL context index. The range is 1-3.
<connectID>	Integer type. SSL connect index. The range is 0-5.
<host_name>	String type. IP address or URL of SSL server.
<port>	Integer type. Port number of remote server.
<connect_mode>	Integer type. Transferring mode of SSL connection. 0 Non-transparent mode 1 Transparent mode
<err>	Integer type. The result of connection. 0 indicates successful operation and any other value indicates an error. Please refer to ***Chapter 4*** for more details.

NOTES

1. Currently only **<connect_mode>**=0 is supported.
2. Currently only **<contextID>**=1 is supported.

2.2.3. AT+QSSLSEND Send Data through SSL Connection

AT+QSSLSEND Send Data through SSL Connection	
Test Command **AT+QSSLSEND=?**	Response **+QSSLSEND: (**range of supported **<contextID>**s**),(** range of supported **<connectID>**s**)[,(**range of supported **<send_length>**s**)]** **OK**
Read Command **AT+QSSLSEND?**	Response **OK**
Write Command Send variable-length data **AT+QSSLSEND=<contextID>,<connectID>**	Response **>** After the above response, the module enters data mode and the data to be sent can be input directly. Tap ″CTRL+Z″ to send the data and tap "ESC" to cancel the operation. If the SSL connection is established and the data is sent successfully: **OK** **+QSSLSEND: <contextID>,<connectID>,<err>** If the SSL connection is not established, disconnected, or some other errors occur: **ERROR**
Write Command Send fixed-length data **AT+QSSLSEND=<contextID>,<connectID>,<send_length>**	Response **>** After the above response, the module enters data mode. After that, type the data to be sent until the data length equals to **<send_length>**. If the SSL connection is established and the data is sent successfully: **OK** **+QSSLSEND: <contextID>,<connectID>,<err>** If the SSL connection is not established, disconnected, or some other errors occur: **ERROR**

Maximum Response Time	**<timeout>** of **AT+QSSLCFG** (default 90s), determined by network
Characteristics	/

Parameter

<contextID>	Integer type. SSL context index. The range is 1-3.
<connectID>	Integer type. SSL connect index. The range is 0-5.
<send_length>	Integer type. The length of the data to be sent. The range is 1-1460 in Text format and 1-730 in Hex format. The data format is determined by **<send_data_format>** in **AT+QSSLCFG=<contextID>,<connectID>,"dataformat"** command.
<err>	Integer type. The result of connection. 0 indicates successful operation and any other value indicates an error. Please refer to ***Chapter 4*** for more details.

NOTES

1. When **<send_data_format>** in **AT+QSSLCFG** is set to 1, the length of the input data after executing **AT+QSSLSEND=<contextID>,<connectID>,<send_length>** must be twice of **<send_length>**.
2. Currently only **<contextID>**=1 is supported.

2.2.4. AT+QSSLCLOSE Close an SSL Connection

The command is used to close an SSL connection. If all SSL connections based on the same SSL context are closed, the module will release the SSL context.

AT+QSSLCLOSE Close an SSL Connection	
Test Command **AT+QSSLCLOSE=?**	Response **+QSSLCLOSE: (**range of supported **<contextID>**s**),(** range of supported **<connectID>**s**)** **OK**
Read Command **AT+QSSLCLOSE?**	Response **OK**
Write Command **AT+QSSLCLOSE=<contextID>,<connectID>**	Response If the SSL connection is closed successfully: **OK** **+QSSLCLOSE: <contextID>,<connectID>,<err>** If there is any error: **ERROR**

Maximum Response Time	300 ms
Characteristics	/

Parameter

<contextID>	Integer type. SSL context index. The range is 1-3.
<connectID>	Integer type. SSL connect index. The range is 0-5.
<err>	Integer type. The result of connection. 0 indicates successful operation and any other value indicates an error. Please refer to ***Chapter 4*** for more details.

NOTE

Currently only **<contextID>**=1 is supported.

2.3. Description of URCs

SSL URCs begin with **+QSSLURC:** and they are mainly used to notify the host to read the received data and to disconnect the connections.

2.3.1. +QSSLURC: "recv" Notify Incoming Data

The URC is used to notify the host of incoming data.

+QSSLURC: "recv" Notify Incoming Data	
+QSSLURC: "recv",<contextID>,<connectID>,<length>,"<data>"	The URC notifies the host of incoming SSL data.

Parameter

<contextID>	Integer type. SSL context index. The range is 1-3.
<connectID>	Integer type. SSL connect index. The range is 0-5.
<length>	Integer type. The length of data. The range is 1-1300 in Text format, and 1-650 in Hex format.
<data>	String type. The data from the module's socket. The maximum length is 1300 bytes.

2.3.2. +QSSLURC: "closed" Notify SSL Connection Disconnected

The URC is used to notify the host that the SSL connection has been disconnected. If this URC is reported, the module will close SSL connection automatically, and the host does not need to execute **AT+QSSLCLOSE** to close the SSL connection.

+QSSLURC: "closed" Notify SSL Connection Disconnected	
+QSSLURC: "closed",<contextID>,<connectID>	The SSL connection based on the specified socket is closed.

Parameter

<contextID>	Integer type. SSL context index. The range is 1-3.
<connectID>	Integer type. SSL connect index. The range is 0-5.

3 Example

3.1. SSL Function of Two-way Authentication

```
AT+QSCLK=0                                  //Disable sleep mode
OK

//Configure certificates and keys
AT+QSSLCFG=1,5,"seclevel",2                 //Manage server and client authentication
OK
AT+QSSLCFG=1,5,"cacert"                     //Configure CA certificate
>                                           //Input the content of the trusted CA certificate in PEM format. Tap "CTRL+Z" to send.

+QSSLCFG: 1,5,"cacert",1216

OK
AT+QSSLCFG=1,5,"clientcert"                 //Configure client certificate
>                                           //Input the content of the client certificate in PEM format. Tap "CTRL+Z" to send.

+QSSLCFG: 1,5,"clientcert",1224

OK
AT+QSSLCFG=1,5,"clientkey"                  //Configure client private key
>                                           //Input the content of the client private key in PEM format. Tap "CTRL+Z" to send.

+QSSLCFG: 1,5,"clientkey",1679

OK
AT+QSSLOPEN=1,5,"hf.quectel.com",8164,0     //Open an SSL server connection
OK

+QSSLOPEN: 1,5,0
AT+QSSLSEND=1,5                             //Send data to SSL server
>                                           //After the response, input the data to be sent and tap "CTRL+Z" to send the data.

OK
```

```
+QSSLSEND: 1,5,0

+QSSLURC: "recv",1,5,10,"1234567890"          //Received data from SSL server
AT+QSSLCLOSE=1,5                              //Close the SSL connection
OK

+QSSLCLOSE: 1,5,0
AT+QSCLK=1                                    //Enable light sleep and deep sleep and wake up by
                                                PSM_EINT (falling edge)
OK
```

4 Error Codes of SSL AT Commands

Table 3: Summary of Error Codes

<err>	Description
0	Operation successful
-1	Exception error
-2	Connection error
-3	Cert error
-4	Key error
-5	Cipher error
-6	State error
-7	Time out
-9	Other errors

5 Appendix A Reference

Table 4: Terms and Abbreviations

Abbreviation	Description
CA	Certificate Authority
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
NB-IoT	Narrowband Internet of Things
PEM	Privacy Enhanced Mail Certificate
SSL	Security Socket Layer
TA	Terminal Adaptor
TLS	Transport Layer Security
UE	User Equipment
URC	Unsolicited Result Code
URL	Uniform Resource Locator