BC26&BC20 SSL 应用指导

NB-IoT 模块系列

版本：BC26&BC20_SSL_应用指导_V1.0

日期：2020-05-28

状态：受控文件

上海移远通信技术股份有限公司始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司
上海市闵行区田林路 1016 号科技绿洲 3 期（B 区）5 号楼　　邮编：200233
电话：+86 21 51086236　　邮箱：info@quectel.com

或联系我司当地办事处，详情请登录：
http://www.quectel.com/cn/support/sales.htm

如需技术支持或反馈我司技术文档中的问题，可随时登陆如下网址：
http://www.quectel.com/cn/support/technical.htm
或发送邮件至：support@quectel.com

前言

上海移远通信技术股份有限公司提供该文档内容用以支持其客户的产品设计。客户须按照文档中提供的规范、参数来设计其产品。由于客户操作不当而造成的人身伤害或财产损失，本公司不承担任何责任。在未声明前，上海移远通信技术股份有限公司有权对该文档进行更新。

版权申明

文档历史

修订记录

版本	日期	作者	变更表述
1.0	2020-05-28	蒋涛/李建	初始版本

目录

表格索引

1 引言

本文档介绍如何使用移远通信 BC26 和 BC20 NB-IoT 模块的 SSL 功能。

为确保通信的私密性，在某些情况下，服务器和客户端之间的通信应采用加密方式，以防止在通信过程中数据被窃听、篡改或伪造。SSL 功能即可满足上述需求。

1.1. SSL 版本

下表为移远通信 BC26 和 BC20 NB-IoT 模块支持的 SSL 版本。

表 1：SSL 版本

SSL 版本
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2

1.2. SSL 加密套件

下表为移远通信 BC26 和 BC20 NB-IoT 模块支持的 SSL 加密套件。有关加密套件的详细说明，请参阅 https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。

表 2：支持的 SSL 加密套件

加密套件代码	加密套件名称（IANA 官方名称）
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 SSL AT 命令详解

2.1. AT 命令语句

2.1.1. 定义

- **<CR>** 回车符。
- **<LF>** 换行符。
- **<…>** 参数名称。实际命令行中不包含尖括号。
- **[…]** 可选参数或 TA 信息响应的可选部分。实际命令行中不包含方括号。若无特别说明，配置命令中的可选参数被省略时，将默认使用其之前已设置的值或其默认值。
- 下划线 参数的默认设置。

2.1.2. AT 命令语句

前缀 **AT** 或 **at** 必须加在每个命令行的开头。输入**<CR>**将终止命令行。通常，命令后面跟随形式为**<CR><LF><response><CR><LF>**的响应。在本文档中，仅显示响应**<response>**，省略**<CR><LF>**。

表 3：AT 命令及响应类型

测试命令	**AT+<cmd>=?**	返回相应设置命令或内部程序可支持的参数取值列表或范围。
查询命令	**AT+<cmd>?**	返回相应设置命令的当前参数设置值。
设置命令	**AT+<cmd>=<p1>[,<p2>[,<p3>[...]]]**	设置用户可自定义的参数值。
执行命令	**AT+<cmd>**	主动执行内部程序实现的功能集。

2.2. AT 命令详解

2.2.1. AT+QSSLCFG 配置 SSL 上下文参数

该命令用于配置 SSL 功能相关的参数，如认证模式、协议版本、发送和接受数据的格式等。

AT+QSSLCFG 配置 SSL 上下文参数	
测试命令 **AT+QSSLCFG=?**	响应 **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**)** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"seclevel"[,(**支持的**<seclevel>**范围**)]** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"sslversion"[,(**支持的**<sslversion>**范围**)]** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"dataformat"[,(**支持的**<send_data_format>**列表**),(**支持的**<recv_data_format>**列表**)]** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"timeout"[,(**支持的**<timeout>**范围**)]** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"debug"[,(**支持的**<debug_level>**范围**)]** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"cacert"** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"clientcert"** **+QSSLCFG: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),"clientkey"** **OK**
设置命令 查询指定上下文的设置： **AT+QSSLCFG=<contextID>,<connectID>**	响应 **+QSSLCFG: <contextID>,<connectID>,"seclevel",<seclevel>** **+QSSLCFG: <contextID>,<connectID>,"sslversion",<sslversion>** **+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",<che**

	cksum> **+QSSLCFG: <contextID>,<connectID>,"clientkey",<checksum>** **OK** 若有任何错误： **ERROR**
设置命令 **AT+QSSLCFG=<contextID>,<connectID>,"seclevel"[,<seclevel>]**	响应 若省略可选参数，则查询指定 SSL 上下文的认证模式： **+QSSLCFG: <contextID>,<connectID>,"seclevel",<seclevel>** **OK** 若指定可选参数，则为指定 SSL 上下文设置认证模式： **OK** 若有任何错误： **ERROR**
设置命令 **AT+QSSLCFG=<contextID>,<connectID>,"sslversion"[,<sslversion>]**	响应 若省略可选参数，则查询指定 SSL 上下文的协议版本： **+QSSLCFG: <contextID>,<connectID>,"sslversion",<sslversion>** **OK** 若指定可选参数，则为指定 SSL 上下文设置协议版本： **OK** 若有任何错误： **ERROR**
设置命令 **AT+QSSLCFG=<contextID>,<connectID>,"dataformat"[,<send_data_format>,<recv_data_format>]**	响应 若省略可选参数，则查询发送/接收数据的格式： **+QSSLCFG: <contextID>,<connectID>,"dataformat",<send_data_format>,<recv_data_format>** **OK** 若指定可选参数，则配置发送/接收数据的格式： **OK** 若有任何错误： **ERROR**

设置命令 **AT+QSSLCFG=<contextID>,<connectID>,"timeout"[,<timeout>]**	响应 若省略可选参数，则查询指定 SSL 上下文的连接和信息发送超时时间： **+QSSLCFG: <contextID>,<connectID>,"timeout",<timeout>** **OK** 若指定可选参数，则配置指定 SSL 上下文的连接和信息发送超时时间： **OK** 若有任何错误： **ERROR**
设置命令 **AT+QSSLCFG=<contextID>,<connectID>,"debug"[,<debug_level>]**	响应 若省略可选参数，则查询指定 SSL 上下文的 Mbed TLS 库调试日志打印等级： **+QSSLCFG: <contextID>,<connectID>,"debug",<debug_level>** **OK** 若指定可选参数，则配置指定 SSL 上下文的 Mbed TLS 库调试日志打印等级： **OK** 若有任何错误： **ERROR**
设置命令 为指定的 SSL 上下文配置 PEM 格式的受信任 CA 证书内容： **AT+QSSLCFG=<contextID>,<connectID>,"cacert"**	响应 **>** 响应 **>**后，模块将在 500 毫秒内进入数据模式；之后即可直接输入待发数据，按 **Ctrl+Z** 发送，按 **Esc** 取消发送。 **+QSSLCFG: <contextID>,<connectID>,"cacert",<checksum>** **OK** 若有任何错误： **ERROR**
设置命令 为指定的 SSL 上下文配置 PEM 格式的客户端证书内容： **AT+QSSLCFG=<contextID>,<connect**	响应 **>** 响应 **>**后，模块将在 500 毫秒内进入数据模式；之后即可直接输入待发数据，按 **Ctrl+Z** 发送，按 **Esc** 取消发送。

ID>,"clientcert"	**+QSSLCFG: <contextID>,<connectID>,"clientcert",<checksum>** **OK** 若有任何错误： **ERROR**
设置命令 为指定的 SSL 上下文配置 PEM 格式的客户端密钥内容： **AT+QSSLCFG=<contextID>,<connectID>,"clientkey"**	响应 **>** 响应 **>**后，模块将在 500 毫秒内进入数据模式；之后即可直接输入待发数据，按 **Ctrl+Z** 发送，按 **Esc** 取消发送。 **+QSSLCFG: <contextID>,<connectID>,"clientkey",<checksum>** **OK** 若有任何错误： **ERROR**
最大响应时间	300 毫秒
特性说明	该命令立即生效。 深休眠唤醒无效；不保存至 NVRAM。

参数

<contextID>	整型。SSL 上下文标识符。范围：1~3。
<connectID>	整型。SSL Socket 标识符。范围：0~5。
<seclevel>	整型。连接认证模式。 0 无认证 1 单向认证 2 双向认证
<sslversion>	整型。连接协议版本。 0 SSL 3.0 1 TLS 1.0 2 TLS 1.1 3 TLS 1.2 4 所有协议均支持，具体使用的协议版本需要同服务器协商
<send_data_format>	整型。发送数据的格式。 0 文本字符号格式 1 十六进制格式
<recv_data_format>	整型。接收数据的格式。

	0 文本字符号格式 1 十六进制格式
<timeout>	整型。连接或消息传输的超时时间。范围：10~300；默认值：90；单位：秒。
<debug_level>	整型。Mbed TLS 库调试日志打印等级。 0 不打印调试日志 1 打印 Error 相关调试日志 2 打印 State 相关调试日志 3 打印 Info 相关调试日志 4 打印 Detail 相关调试日志
<checksum>	整型。输入证书的总字节数，可用于本地校验。

备注

1. 目前仅支持**<contextID>**=1。
2. **<debug_level>**仅可在调试时使用；且设置等级越高（即参数值越大），获取到的日志就越多。
3. 若**<seclevel>**=0，则无需配置任何证书或密钥；若**<seclevel>**=1，则需配置 CA 证书；若**<seclevel>**=2，则需配置 CA 证书、客户端证书和客户端密钥。
4. 在数据模式下发送数据时，建议返回 **>** 后等待 500 毫秒再发送数据。

2.2.2. AT+QSSLOPEN 建立 SSL 连接

该命令用于建立 SSL 连接。

AT+QSSLOPEN 建立 SSL 连接	
测试命令 **AT+QSSLOPEN=?**	响应 **+QSSLOPEN: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**),<host_name>,<port>,(**支持的**<connect_mode>**列表**)** **OK**
查询命令 **AT+QSSLOPEN?**	响应 **OK**
设置命令 **AT+QSSLOPEN=<contextID>,<connectID>,<host_name>,<port>,<connect_mode>**	响应 **OK** **+QSSLOPEN: <contextID>,<connectID>,<err>** 若有任何错误： **ERROR**
最大响应时间	由 **AT+QSSLCFG** 的**<timeout>**决定（默认 90 秒），且受网络影响

特性说明	/

参数

<contextID>	整型。SSL 上下文标识符。范围：1~3。
<connectID>	整型。SSL Socket 标识符。范围：0~5。
<host_name>	字符串类型。SSL 服务器的 IP 地址或者域名。
<port>	整型。远程服务器的端口号。
<connect_mode>	整型。数据传输模式。 0 非透传模式 1 透传模式
<err>	整型。连接结果。详情请参考***第 4 章***。 0 执行成功 其他值 执行失败

备注

1. 目前仅支持**<contextID>**=1。
2. 目前仅支持**<connect_mode>**=0。

2.2.3. AT+QSSLSEND 发送数据

AT+QSSLSEND 发送数据	
测试命令 **AT+QSSLSEND=?**	响应 **+QSSLSEND: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**)[,(**支持的**<send_length>**范围**)]** **OK**
查询命令 **AT+QSSLSEND?**	响应 **OK**
设置命令 发送不定长数据 **AT+QSSLSEND=<contextID>,<connectID>**	响应 **>** 响应 **>**后，模块将在 500 毫秒内进入数据模式；之后即可直接输入待发数据，按 **Ctrl+Z** 发送数据，按 **Esc** 取消发送。 若 SSL 数据发送成功： **OK** **+QSSLSEND: <contextID>,<connectID>,<err>**

	若 SSL 未连接、连接断开或者其他错误： **ERROR**
设置命令 发送定长数据 **AT+QSSLSEND=<contextID>,<connectID>,<send_length>**	响应 **>** 响应 **>**后，模块将在 500 毫秒内进入数据模式；之后即可输入长度等于**<send_length>**的待发数据。 若 SSL 数据发送成功： **OK** **+QSSLSEND: <contextID>,<connectID>,<err>** 若 SSL 未连接、连接断开或者其他错误： **ERROR**
最大响应时间	由 **AT+QSSLCFG** 的**<timeout>**决定（默认 90 秒），且受网络影响
特性说明	/

参数

<contextID>	整型。SSL 上下文标识符。范围：1~3。
<connectID>	整型。SSL Socket 标识符。范围：0~5。
<send_length>	整型。待发送数据的长度。单位：字节。 文本字符串格式下范围：1~1460；十六进制格式下范围：1~730。 数据格式由 **AT+QSSLCFG=<contextID>,<connectID>,"dataformat"** 中的**<send_data_format>**指定。
<err>	整型。连接结果。详情请参考***第 4 章***。 0 执行成功 其他值 执行失败

备注

1. 当 **AT+QSSLCFG** 中的**<send_data_format>**设置为 1（十六进制格式），执行 **AT+QSSLSEND=<contextID>,<connectID>,<send_length>**后输入的数据长度必须是**<send_length>**的两倍。
2. 目前仅支持**<contextID>**=1。
3. 在数据模式下发送数据时，建议返回 **>** 后等待 500 毫秒再发送数据。

2.2.4. AT+QSSLCLOSE 断开 SSL 连接

该命令用于断开 SSL 连接。若同一个 SSL 上下文的所有 SSL Socket 连接都已断开，则模块将释放该 SSL 上下文。

AT+QSSLCLOSE 断开 SSL 连接	
测试命令 **AT+QSSLCLOSE=?**	Response **+QSSLCLOSE: (**支持的**<contextID>**范围**),(**支持的**<connectID>**范围**)** **OK**
查询命令 **AT+QSSLCLOSE?**	响应 **OK**
设置命令 **AT+QSSLCLOSE=<contextID>,<connectID>**	响应 如果 SSL 连接被成功关闭： **OK** **+QSSLCLOSE: <contextID>,<connectID>,<err>** 若有任何错误： **ERROR**
最大响应时间	300 毫秒
特性说明	/

参数

<contextID>	整型。SSL 上下文标识符。范围：1~3。
<connectID>	整型。SSL Socket 标识符。范围：0~5。
<err>	整型。连接结果。详情请参考***第 4 章***。 0 执行成功 其他值 执行失败

备注

目前仅支持**<contextID>**=1。

2.3. URC 详解

SSL 相关的 URC 以**+QSSLURC:**开头，主要用于通知 MCU 收到新数据或 SSL 连接状态改变。

2.3.1. +QSSLURC: "recv" 通知 MCU 接收到新数据

该 URC 用于通知 MCU 接收到新数据。

+QSSLURC: "recv" 通知 MCU 接收到新数据	
+QSSLURC: "recv",<contextID>,<connectID>,<length>,<data>	通知 MCU 接收到新数据

参数

<contextID>	整型。SSL 上下文标识符。范围：1~3。
<connectID>	整型。SSL Socket 标识符。范围：0~5。
<length>	整型。数据长度。单位：字节。 文本字符串格式范围：1~1300；十六进制格式下范围：1~650。
<data>	字符串类型。模块接收的业务数据。最大长度：1300 字节。

2.3.2. +QSSLURC: "closed" 通知 MCU SSL 连接将断开

该 URC 用于通知 MCU SSL 连接将断开。上报此 URC 后，模块将立即自动关闭 SSL 连接，MCU 无需再执行 **AT+QSSLCLOSE**。

+QSSLURC: "closed" 通知 MCU SSL 连接将断开	
+QSSLURC: "closed",<contextID>,<connectID>	基于指定 Socket 的 SSL 连接将断开。

参数

<contextID>	整型。SSL 上下文标识符。范围：1~3。
<connectID>	整型。SSL Socket 标识符。范围：0~5。

3 举例

3.1. 双向认证的 SSL 功能

```
AT+QSCLK=0                                  //禁用模块的休眠模式
OK

//配置证书和密钥
AT+QSSLCFG=1,5,"seclevel",2                 //配置认证方式为双向认证
OK
AT+QSSLCFG=1,5,"cacert"                     //配置 CA 证书
>                                           //输入 PEM 格式的 CA 证书内容，按 Ctrl+Z 发送

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

OK
AT+QSSLCFG=1,5,"clientcert"                 //配置客户端证书
>                                           //输入 PEM 格式的客户端证书内容，按 Ctrl+Z 发送

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

OK
AT+QSSLCFG=1,5,"clientkey"                  //配置客户端密钥
>                                           //输入 PEM 格式的客户端密钥，按 Ctrl+Z 发送

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

OK
AT+QSSLOPEN=1,5,"hf.quectel.com",8164,0     //建立 SSL 连接
OK

+QSSLOPEN: 1,5,0
AT+QSSLSEND=1,5                             //发送数据
>                                           //输入要发送的数据，按 Ctrl+Z 发送

OK
```

```
+QSSLSEND: 1,5,0

+QSSLURC: "recv",1,5,10,"1234567890"      //通知 MCU 接收到新数据
AT+QSSLCLOSE=1,5                          //关闭 SSL 连接
OK

+QSSLCLOSE: 1,5,0
AT+QSCLK=1                                //启用轻休眠和深休眠，并可通过 PSM_EINT（下降沿）
OK                                        唤醒深休眠
```

4 错误码

表 4：错误码概览

<err>错误码	英文描述	中文描述
0	Operation successful	执行成功
-1	Exception error	异常错误
-2	Connection error	连接失败
-3	Cert error	配置 CA 证书或客户端证书错误
-4	Key error	配置客户端密钥错误
-5	Cipher error	配置加密套件错误
-6	State error	状态错误
-7	Time out	执行超时
-9	Other errors	其他错误

5 附录 A 参考文档和术语缩写

表 5：术语缩写

缩写	英文全称	中文全称
CA	Certificate Authority	证书授权中心
IANA	Internet Assigned Numbers Authority	互联网号码分配局
ID	Identifier	标识符
IP	Internet Protocol	互联网协议
MCU	Microprogrammed Control Unit	微程序控制器
NB-IoT	Narrowband Internet of Things	窄带物联网
NVRAM	Non-Volatile Random Access Memory	非易失性随机访问存储器
PEM	Privacy Enhanced Mail	隐私增强邮件
SSL	Security Socket Layer	安全套接层
TA	Terminal Adapter	终端适配器
TLS	Transport Layer Security	安全网络传输协议
URC	Unsolicited Result Code	非请求结果码