User Guide

Pinnacle™ Modem AT Interface Application

V1.11

The scope of this guide relates to a general purpose smartBASIC application for Laird's Pinnacle™ (and compatible) Cellular LTE and Bluetooth Low Energy modem that allows the module to communicate over cellular networks over CAT-M1 or NB-IoT and advertise, scan, and connect via BLE. For BLE, It also offers GATT client and server capabilities in a single application controlled with the industry standard AT command protocol over a UART interface.

This guide also provides a BLE Virtual Serial Port interface that bridges a streaming wireless connection to the cellular functionality built into the Pinnacle™ modem which is also compliant to the 3GPP AT interface for cellular modems.

REVISION HISTORY

Version	Date	Notes	Contributor(s)	Approver
0.8	14 Sep 2018	Draft Release forked from BL65x guide		Mahendra Tailor
0.82	08 Feb 2019	Reflects functionality as per v0.82	Mahendra Tailor	Jonathan Kaye
0.84	18 Feb 2019	Reflects functionality as per v0.84	Mahendra Tailor	Jonathan Kaye
0.88	21 Feb 2019	Reflects functionality as per v0.88	Mahendra Tailor	Jonathan Kaye
0.908	25 Mar 2019	Reflects functionality as per v0.908	Mahendra Tailor	Jonathan Kaye
1.02	17 June 2019	Production release	Mahendra Tailor	Jonathan Kaye
1.10	23 Sep 2019	Added VG/G2/G6/Ds/AX async responses	Mahendra Tailor	Jonathan Kaye
1.11	11 Feb 2020	Updated Interconnect Diagram Formatting (Doc Team)	Mahendra Tailor	Jonathan Kaye

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

TABLE OF CONTENTS

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

1 OVERVIEW

This document is a user guide for the AT Interface *smart*BASIC application written for the Pinnacle™ Cellular and Bluetooth Low Energy Modem that exposes an AT command/response protocol via a UART interface or a BLE virtual serial port connection.

The AT protocol instructs the modem, on the cellular side to send and receive data to the internet cloud using the LTE CAT-M1 or NB-IoT cellular network and on the Bluetooth side to advertise, scan, connect, and pair. On the Bluetooth side the *smart*BASIC application exposes custom AT commands that enable the creation of a GATT server table and, conversely, enables it to be a GATT client to interact with remote GATT servers over a BLE connection.

It also provides commands to read and write to GPIO pins and additional commands to interact with the NFC radio so that Type 2 tags can be programmed for an NFC reader to access.

The module may also operate as a single connection virtual serial port device for the transparent serial communication between a BLE enabled remote device and the cellular modem embedded in the modem. This occurs in a similar manner as the old AT modems used for data communications on telephone lines.

This application requires that:

- The Pinnacle™ 100 is updated to version 120.3.3.13 or newer firmware
- The AT Interface smartBASIC application (or appropriate variant) has been loaded into the module

1.1 Usage Warning

Please be aware that the Pinnacle modem consists of a cellular modem and a Bluetooth Low Energy SoC. The latter has two UART peripherals. One is exposed to the external host and the other is internally connection to the UART of the cellular modem.

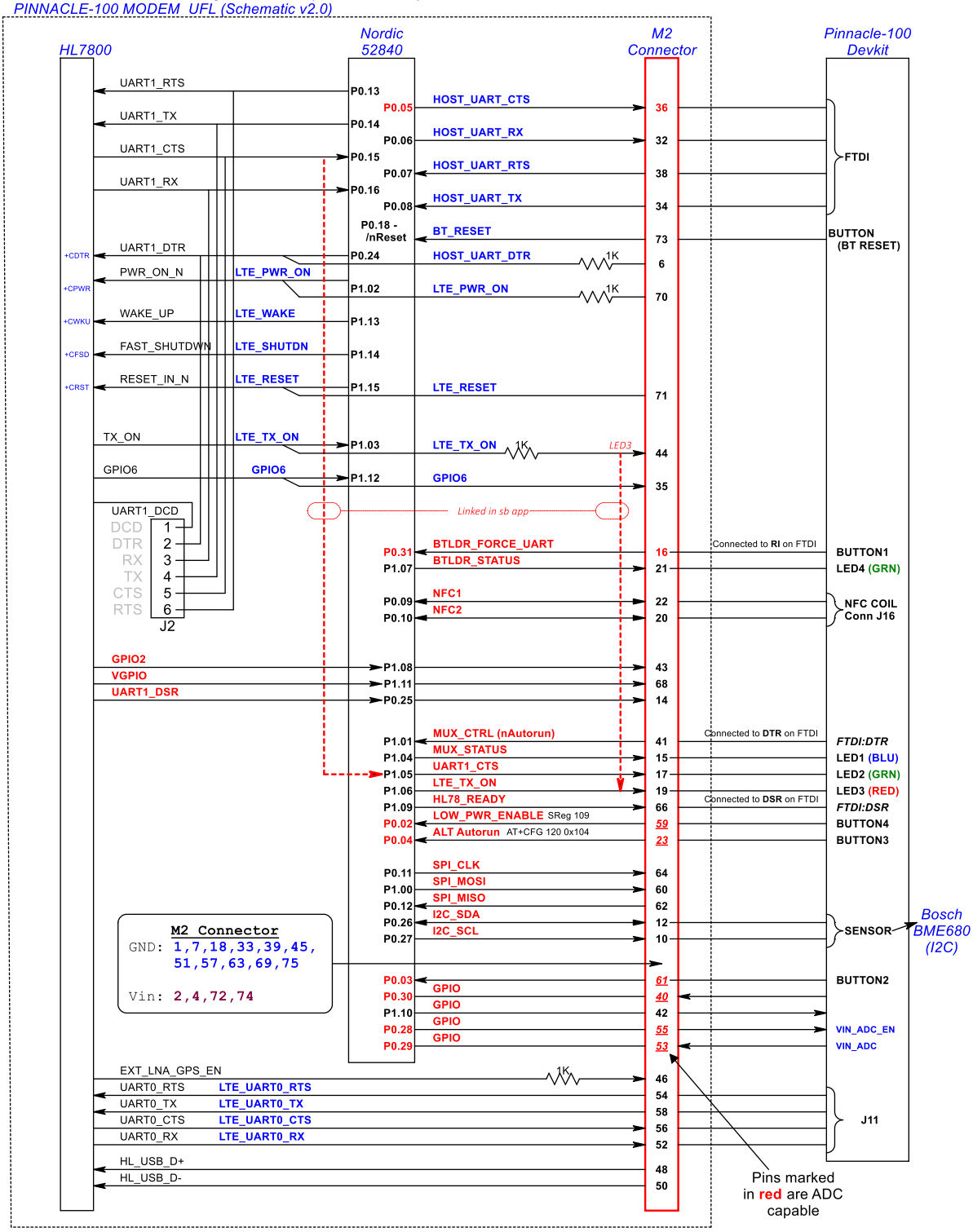
This means that AT commands meant for the cellular modem are bridged via firmware in the SoC. This means that the baud rates for the two UARTs in the SoC can be different, however, by default they are both configured to have the same baudrate and parameters such as parity and stop bits.

The host should be aware of this arrangement when sending AT commands to the cellular modem because there are some commands that could change the baudrate or handshaking functionality. Appropriate commands must be sent to the SoC to configure the second UART interface appropriately and then finally reflected on to the UART to which the host is talking. See commands AT+AUXC and AT+URTC to expedite those changes.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

2 PINNACLE-100 SIGNAL INTERCONNECTION (HOSTED MODE)

PINNACLE-100 MODEM Integrated Antena (Schematic v5.0)
PINNACLE-100 MODEM UFL (Schematic v2.0)



Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

2.1 M2 Connector Pin Functions

This section provides details about some of the pins on the M2 connector.

Table 1: M2 connector pin functions

Pin	Description
36,32,38,34	Host UART connection. CTS, RX, RTS, and TX respectively.
73	**BT RESET** A low asserts RESET on the nrf52840 microcontroller (the modem is not reset. See pin 71 for that.)
70	**LTE POWER ON** Directly connected to the PWR_ON_N pin of the HL7800 modem and also to output pin P1.02 of the nrf52840 microcontroller. Hence the PWR_ON_N pin of the HL7800 can be affected either by driving pin M2.70 or by the AT+CPWR command.
71	**LTE RESET** Directly connected to the RESET_IN_N pin of the HL7800 modem and also to output pin P1.15 of the nrf52840 microcontroller. Hence the RESET_IN pin of the HL7800 can be affected either by driving pin M2.71 or by the AT+CRST command. **Note:** This pin does not reset the nrf52840 microcontroller. Use Pin 73 for that. **Warning:** Use the AT+CRST command (and not this physical line) to assert HL7800 reset. Using the physical line confuses the algorithm in the *smart*BASIC application that monitors the state of the HL7800. When this line is externally asserted low, the application is not aware that the HL7800 was reset and so the AT+CCMS command returns a false indication.
44	**LTE TX ON** This pin is directly driven by TX_ON pin of the HL7800 modem and is asserted when it is transmitting on the cellular radio. See the HL7800 datasheet for more details.
35	**GPIO6** This pin is directly driven by GPIO6 pin of the HL7800 modem and used during eDRX mode to indicate to the host that there has been some activity that needs to be reported. See the HL7800 datasheet for more details.
16	**BTLDR_FORCE_UART** This pin is checked at start-up by the Laird bootloader. If held low at start-up or during reset of the module (must be held low for a minimum of X ms to be correctly detected) the bootloader is entered, and a firmware upgrade can take place over UART using the utilities provided. No external pull-up resistor is required for this pin as it is pulled high by the module at start-up. After the main application has booted, this pin can be used as a GPIO pin although Laird recommends that this pin should be dedicated for entering the bootloader only; if the Laird bootloader is not used and erased then this pin can be safely used for any purpose.
21	**BTLDR_STATUS** This pin is used as an output by the bootloader to indicate the current status of the bootloader or module start-up and should be connected to an LED (via a logic gate which can supply the required voltage and current). After the main application has booted, this pin can be used as a GPIO pin although Laird recommends that this pin should be dedicated for bootloader status indication only; if the Laird bootloader is not used and erased then this pin can be safely used for any purpose. Pin status is as follows: ▪ Smooth pulsing – In UART bootloader awaiting activation command ▪ 3 pulses – Receiving data via UART or waiting for command via UART ▪ 4 pulses – Reading/processing update data ▪ 5 pulses – Update in progress ▪ Always on – Fatal error has occurred (module boot cannot proceed)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Pin	Description
20,22	This is where the NFC coil is attached. NFC functionality is exposed by the nrf52840 microcontroller via appropriate AT commands which are described later in this document. It is possible to configure the nrf52840 microcontroller so that these two pins are plain GPIO. However, that is a one-time configuration and, once configured, NFC functionality cannot be reinstated until after chip-erasing the nrf52840 microcontroller and reloading the firmware.
43	**GPIO2** This pin is directly driven by GPIO2 pin of the HL7800 modem. See the HL7800 datasheet for more details.
68	**VGPIO** This pin is directly driven by VGPIO pin of the HL7800 modem and is low when the HL7800 modem is in hibernate mode. See the HL7800 datasheet for more details.
14	**UART1_DSR** This is driven by the DSR output line of the UART1 interface of the HL7800 modem. It is an output line because the HL7800 modem is a DCE device.
41	**MUX CONTROL** This pin is used in multiplexer modes 0 and 1 to specify where AT commands are delivered – either to the nrf52840 or the HL7800. On the Pinnacle dev kit, this pin is connected to the DTR output of the FTDI USB to serial chip. This means that it enables where AT commands are delivered by asserting and deasserting the DTR output of the host. ▪ In Mode 0 – If this pin is low, then all UART data is delivered to the HL7800; if high then UART data is delivered to the nrf52840 microcontroller. ▪ In Mode 1 – Low to high transitions are used to flip the multiplexer output from the HL7800 to the nrf52840 and vice versa. At any time, the state of pin 15 indicates the current direction of the output of the multiplexer. **Note:** If the *smart*BASIC application is replaced and the autorun is not relocated to M2.33 by setting the *smart*BASIC config key 120 using the function NvCfgKeySet() to 33, then the autorun function does not work on this pin but on the current content of the cfg key 120.
15	**MUX STATUS** When this pin is high, it indicates that the multiplexer is currently routing all UART data to the HL7800 modem. When low, all data is routed to the nrf52840 microcontoller.
17	**UART1_CTS ECHO** This pin echoes the state of the UART1_CTS output pin of the HL7800
19	**LTE TX ON ECHO** This pin echoes the state of the TX_ON output pin of the HL7800 and is provided purely so that LED2 on the Pinnacle devkit can indicated the status of that line
66	**HL78_READY** When this pin is logic 0, it indicates that the HL7800 modem is ready to accept AT commands. It is at logic 1 immediately after reset.
59	**UART LOW POWER ENABLE** This pin is used by the host to control the low power operation of the nrf52840 microcontroller. When it is held high, the low UART ports in the microcontroller are always forced to the open state. However, when held low, it informs the microcontroller that it can close the two UARTs if there is no activity on those ports. The inactivity time is set by S Register 213 and by default is set to five seconds. When the UARTs are open, the nrf52840 consumes roughly 300 to 400 microAmps.
23	**ALT AUTORUN** This pin, when held high, ensures that after the nrf52840 chip comes out of reset (pin 73), it automatically launches the ATinterface *smart*BASIC application.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Pin	Description
	Ensure this pin is held high for normal operation and only needs to be pulled low to replace the *smart*BASIC application as per the instructions in the section here.
64	Nominally dedicated for SPI_CLK. Hosted mode currently does not touch these pins.
60	Nominally dedicated for SPI_MOSI. Hosted mode currently does not touch these pins.
62	Nominally dedicated for SPI_MISO. Hosted mode currently does not touch these pins.
12	Nominally dedicated for I2C_SDA. Hosted mode currently does not touch these pins.
10	Nominally dedicated for I2C_SCL. Hosted mode currently does not touch these pins.
55	Nominally dedicated for VIN_ADC_EN on the Pinnacle 100 devkit
53	Nominally dedicated for VIN_ADC on the Pinnacle 100 devkit
46	**EXT_LNA_GPS_EN** This pin is directly driven by EXT_LNA_GPS_EN pin of the HL7800 modem and is asserted when the GPS radio is acquiring location packets. See the HL7800 datasheet for more details.
54,58.56,52	Directly connected to the four UART0 lines of the HL7800 modem.
48,50	Directly connected to the two USB D+/D- lines of the HL7800 modem. For future use.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3 OPERATION

3.1 UART Multiplexer Modes

This application provides mutually-exclusive modes of operation on startup depending on the value of S register 120 which configures the routing behavior of host data arriving via UART0 in Figure 1.

In factory default mode, Sreg 120 contains 1 which means that any data from the HOST is presented to UART 1. This in turn is connected to the cellular modem onboard the module.

To send AT commands to the application processor that exposes BLE and NFC functionality, send the following escape sequence:

```
<delay> ! <delay> ! <delay> ! <delay>
```

This flip switches SWB or toggles the M2.41 twice so that all susequent AT commands are presented to the application processor's AT command processor.

To send AT commands to the HL7800 modem when the mutliplexer is pointing to the 840, send the command **`AT!`**. This results in SWB being flipped back to HL7800.

Refer to the section on ATS and Sregister 120 for more details of other multiplexer modes.

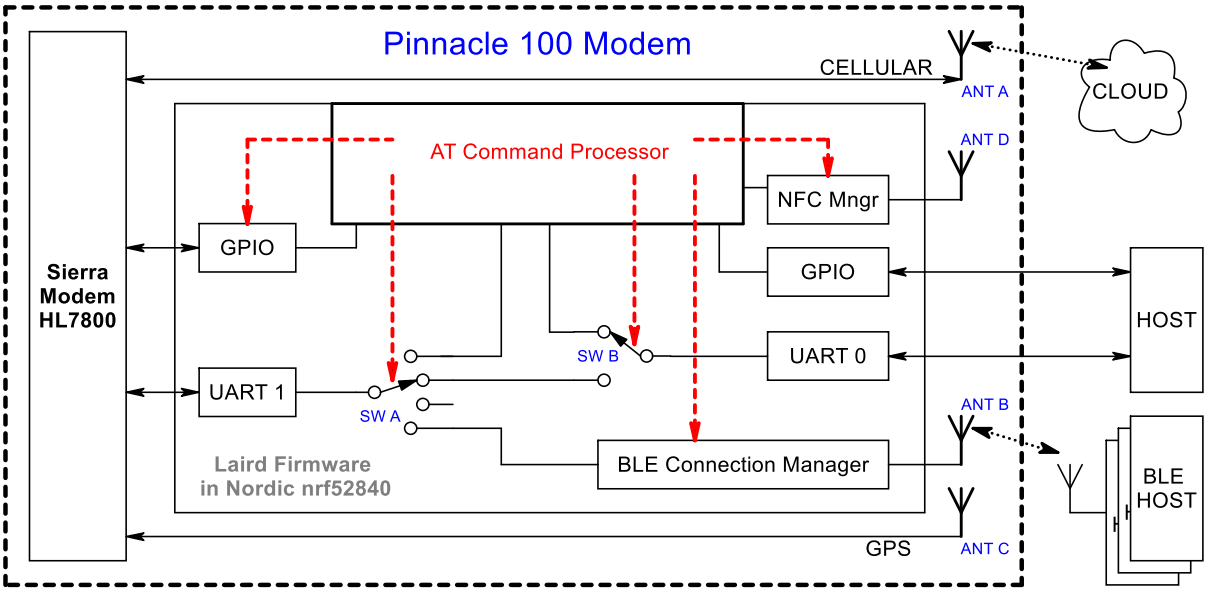


Figure 1: The HL7800 can flow to/from one of three sources

The diagram shows that data for the HL7800 can be arranged to flow to and from one of three sources:

- The host on UART 0
- Internally from the Nordic nrf52840
- A host at the other end of a BLE VSP connection (only in modes 1 and 2)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.2 BLE Operation Modes

This application provides two mutually exclusive modes of operation on startup depending on the value of S register 100 (referred to as VSP and non-VSP modes).

In VSP mode (the default), where bit 0 of S register 100 is set, the application initializes the GATT server table by populating it with the VSP service (and the mandatory GAP and GATT services). It then starts advertising to welcome incoming connections **from trusted devices only by default** but can be disabled via S Register 102. Once connected, data to/from the VSP service is bridged to the auxiliary serial port which is connected to the cellular modem in the module. While there is no connection, AT commands are parsed and actioned (such as the ATD command to initiate an outgoing connection). The auxiliary serial port is bridged to the VSP service only on connection, either incoming or outgoing.

In the non-VSP mode, where bit 0 is not set, the GATT table only contains the mandatory GAP and GATT services. Provided GATT server-related AT commands are used to add services and their characteristics and descriptors. In addition, depending on the states of bits 1 and 2 of S register 100, the module automatically starts advertising and/or scanning. In this mode, it is possible to start/stop advertising and scanning as required and to accept or make connections. Once connected, the AT parser is still active, so it is possible to restart adverts or make further connections. In connected states, it is possible to send GATT client-related commands to interact with a slave device. Note that in this mode virtually all commands are non-blocking, meaning an OK or ERROR response is sent immediately after the command is processed, followed by one or more asynchronous messages. All of the asynchronous responses start with a unique two-letter sequence and so can be demultiplexed and actioned appropriately by the host.

Note: If scanning is enabled, the UART host should expect asynchronous (that is, arrive anytime) responses which contain advert reports. These could be intermixed with normal responses. For this reason, every response type in the Response section has a unique two-letter (case-sensitive) start which allows the host to demultiplex them appropriately.

3.3 Data Flow Control

The host that is driving the UART interface must strictly adhere to RTS/CTS handshaking to ensure that data buffering and management are not compromised. If the module de-asserts its RTS line, the host stops sending data as soon as possible and, conversely, if the host de-asserts its RTS line, the module stops sending data to it.

3.4 AT Commands

These are text commands starting with the character sequence AT and terminated by a \r character (ASCII code 0x0D). Commands are not case sensitive (apart from multiplexing mode 2 where the case of the AT characters determines whether it is forwarded to the cellular modem chipset) and have zero or more parameters. Multiple parameters are separated by the comma (,) character and some commands tolerate empty fields (two consecutive commas) and provide a default value. If more than the specified parameters are supplied, then the extra parameters are either silently ignored or result in a syntax error response.

The UART receive ring buffer has a default non-zero size which is at least 256 bytes long. It is imperative that any command, which is terminated by a \r is not larger than this. Otherwise the system locks since the RTS is de-asserted and the host is unable to send the \r to empty the buffer. The size of the UART RX buffer can be modified using the S register 203.

The concept behind the application is that the host sends AT commands to perform various actions like advertise, scan, connect, pair, get local information, set configuration values, GATT read, and GATT write.

These AT commands are described in this section in alphabetical order. Also listed are responses to these commands which are described in the next chapter.

Many commands take parameters which are either integer values, strings, or hex strings:

- Integer values – Can be entered as binary or in hexadecimal using the syntax 0xhh..hh
- Hex strings – Only contain the letters 0-9,A-F and a-f and shall be exactly an even number long. Otherwise they are treated as syntax errors

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Note: In the following command, there is a space between the AT command and the parameters it accepts. That space is not mandatory; it's only used for visual clarity. In the section heading, the format it **XXXXX (some comment)** please note that the **(some comment)** is not actually part of the comment but a brief description.

[Empty Line]

Command	`//Empty line with 0 or more whitespace//`
Possible Responses	`OK`

AT

Command	**`AT`**
Description	No action performed other than to send the OK response
Possible Responses	`OK`

AT! (Uart to HL7800)

Command	**`AT!`**
Description	If the modem is in multiplexer mode 1 as set in SReg 120 then this command will toggle an internal logical switch so that all subsequent host UART traffic is relayed to the HL7800 modem. To toggle that internal logical switch so that AT commands are again processed by the application microcontroller, send the !!! escape seqeunce descibed below.
Possible Responses	`OK` `+CME ERROR: n`

! ! ! (Uart to 840)

Escape Sequence	`<delay>`**`!`**`<delay>`**`!`**`<delay>!<delay>`
Description	If the modem is in multiplexer mode 1 as set in SReg 120 and the command AT! was used to divert all host traffic to the HL78 modem, then this escape seqence will toggle an internal logical switch so that all susequent AT commands are processed by the application processor.
	Note: There shall be delays of at least X milliseconds on either side of the ! character where X is the value set in S Register 124 and the default is set at 125 milliseconds.
Possible Responses	`OK` `+CME ERROR: n`

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT%S (Read/Write/Query String Registers)

Command

AT%S n="string"

AT%S n?

AT%S n=?

Description

These commands are to set, get, and get the range of valid lengths of the strings of any string valued S Register respectively where the S register is identified by the integer value n.

- ***string*** – When setting, *string* is the new value; the double quotes are mandatory. To embed a non-printable character in the string, escape it using the three-character \hh sequence where hh is the ASCII value of the character in hexadecimal. For example, to filter the six-byte null terminated string Hello, the string is entered as *Hello\00*.
- ***n?* and *n=?*** – For these variants, the returned value is enclosed in \n and \r and are sent before the OK. The two integer values returned by *n=?* are separated by a comma.

Note: When setting the value, it is not retained over a power cycle or a warm reset triggered using the ATZ command. See the AT&W command to make all changed values permanent.

The following S Registers are defined:

Register	Description
0	*Device Name* The length is between 1 and 20
1	*VSP Service Base 128-bit UUID* The length is exactly 32 characters, all hex digits.
2	*Scan Pattern* The length is between 0 and 20 This string specifies a pattern for filtering incoming advert report via scans. If the advert report contains at least one match, then it is reported to the host via the UART. For example, it can be set to the device name of a device and in that case, only that device's adverts are sent to the host. Use the three-character sequence \hh to enter a non-printable character in the string.

Possible Responses

AT&F (Reset to Factory defaults)

Command

AT&F

Description

Clear all S register settings back to defaults *and* clear the trusted device database and then perform a warm reset.

Possible Responses

```
OK (after the warm reset)
+CME ERROR: n
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT&W (Save S registers to non-vol memory)

Command	**AT&W**
Description	Save all S registers to non-volatile memory.
Possible Responses	OK +CME ERROR: n

AT+AARA (Add AD element to advert report)

Command	**AT+AARA tag,"payload"**
Description	<tag> can take the range of 0..255 This command is used to add an AD element with tag and payload specified to the advert report cache variables for adverts that are used when operating in non-vsp mode. To add to the scan report, use *AT+ASRA*. This does not affect the adverts that are already committed to the radio and can be called multiple times to add more AD elements. To commit to the radio, use the *AT+ACMT* command.
Possible Responses	OK +CME ERROR: n

AT+ACMT (NonVsp advert and scan reports cache commit)

Command	**AT+ACMT**
Description	The non-vSP advert and scan report caches created using AT+ARST, AT+AARA, and AT+ASRA are committed for transmission by the radio
Possible Responses	OK +CME ERROR: n

AT+ARST (NonVsp advert and scan reports cache clear)

Command	**AT+ARST <conn>**
Description	<conn> can take the range 0..1 Used to clear the advert and scan report cache variables for adverts that are used when operating in non-vSP mode. This does not affect the adverts that are already committed to the radio.
Possible Responses	OK +CME ERROR: n

AT+ASLP (Config HL78 sleep mode via WAKE and DTR gpio)

Command	**AT+ASLP <0|1>**
Description	Used to allow or disallow the HL78 from entering sleep mode. When set to 1 the HL78 can go into sleep mode when conditions are right. Otherwise when set to 0 it prevents the HL78 from entering sleep. When the value is 0, the WAKE_UP line is set to 1 and DTR line is set to 0 When the value is 1, the WAKE_UP line is set to 0 and DTR line is set to 1
Possible Responses	OK +CME ERROR: n

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+ASRA (Add AD element to scan report)

Command	**AT+ASRA tag,"payload"**
Description	<tag> can take the range 0..255 Used to add an AD element with tag and payload specified to the scan report cache variables for adverts that are used when operating in non-vSP mode. To add to the advert report, use *AT+AARA*. This does not affect the adverts that are already committed to the radio and can be called multiple times to add more AD elements. To commit to the radio, use the *AT+ACMT* command.
Possible Responses	OK +CME ERROR: n

AT+AUXC (Config baud+flow of 840 uart connected to HL7800)

Command	**AT+AUXC baud,flow**
Description	Close and re-open the auxilliary port with the baud rate and optional CTS/RTS flow control specified ▪ 0 - None ▪ 1 – CTS/RTS flow control It is valid to have the auxilliary and main UART port to be at different baud rates. To non-persistantly change operation of the main port use the command AT+URTC.
Possible Responses	OK +CME ERROR: n

AT+BNDD (Delete entry in BLE trusted device database)

Command	**AT+BNDD address**
Description	Use this command to delete a device from the trusted device database.
Possible Responses	OK +CME ERROR: n

AT+BNDP (Convert entry in BLE trusted database from rolling to persistent)

Command	**AT+BNDP address**
Description	When a pairing is successful, the pairing keys and address are stored in the trusted device database and are marked as a **rolling** type. If the database is full, to guarantee storage of the newest pairing, the oldest rolling record is automatically deleted to make space. User this to change the type of record to **persistent** so it can only be deleted if explicitly done using the AT+BNDD command. *Please note that both type are non-volatile*.
Possible Responses	OK +CME ERROR: n

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+BNDT (Check if address is a BLE trusted device)

Command **AT+BNDT address**

Description Checks if a device identified by *address* (a 14-digit hex string) is present in the trusted device database (a result of a successful pairing).

The following response is sent before the OK if it is not trusted:

```
\n0\r
```

If trusted, the response is:

```
\n1,t,14digithexaddr\r
```

…where *t* is 0 if the pairing is persistent and !0 if rolling.

Note: *Rolling* means that, at some point, it could be automatically deleted on a new pairing if the database is full.

14digithexaddr is the actual MAC address of the device if the *address* passed to this command is a resolvable address.

At any time, the command ATI2009 returns the number of devices in the trusted device database.

Possible Responses

```
OK
+CME ERROR: n
```

AT+BNDX (Delete all addresses in trusted device database)

Command **AT+BNDX**

Description Use this command to delete all devices from the trusted device database, both rolling and persistent types.

Possible Responses

```
OK
+CME ERROR: n
```

AT+CCMS (Query power state of HL7800)

Command **AT+CCMS**

Description Use this command to query the current state of the HL7800. This is a value from 0 to 4.

- 0 – When the HL7800 is coming out of reset, which takes many seconds, signifies that it is not ready to accept AT commands.
- 1 – RUN state
- 2 – SLEEP state
- 3 – Lite Hibernate state
- 4 – Hibernate state which is the lowest power consumption state

Note: This is a future command and should not be relied upon until if this note is present.

Possible Responses

```
OK
+CME ERROR: n
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+CDTR (Set HL7800's DTR input pin)

Command	**AT+CDTR state**
Description	Sets the output state of the DTR input pin of the cellular modem chipset as per *state* which can be either 0 or 1. Since the cellular modem is a DCE, its DTR line is an input and so an output from the application MCU.
Possible Responses	OK +CME ERROR: n

AT+CPWR (Set HL7800's PWR_ON_N input pin)

Command	**AT+CPWR state**
Description	Sets the output state of the PWR_ON_N input pin of the cellular modem chipset as per *state* which can be either 0 or 1. See datasheet for the HL7800 for more details.
Possible Responses	OK +CME ERROR: n

AT+CWKU (Set HL7800's WAKE_UP input pin)

Command	**AT+CWKU state**
Description	Sets the output state of the WAKE_UP input pin of the cellular modem chipset as per *state* which can be either 0 or 1. See datasheet for the HL7800 for more details.
Possible Responses	OK +CME ERROR: n

AT+CFSD (Set HL7800's FAST_SHUTDWN_N input pin)

Command	**AT+CFSD state**
Description	Sets the output state of the FAST_SHUTDOWN_N input pin of the cellular modem chipset as per *state* which can be either 0 or 1. See datasheet for the HL7800 for more details.
Possible Responses	OK +CME ERROR: n

AT+CRST (Set HL7800's RESET_IN_N input pin)

Command	**AT+CRST timeMs**
Description	Sets the output state of the RESET_IN_N input pin of the cellular modem chipset low for the time specified in the range 0 to 500 milliseconds, unless the value of *timeMs* is 0 or 1. When *timeMs* is 0, then the RESET_N pin is held low until the command is sent again with *timeMs* set to 1 or, if more than 1, then it holds it low for a further time specified by *timeMs* and then set to high.
Possible Responses	OK +CME ERROR: n

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+CSTS (Query counts of level changes of VGPIO, GPIO2,GPIO6,URT1_DSR)

Command	**AT+CSTS n**
Description	Gets the number of times HL78 output pins VGPIO, GPIO2, GPIO6, UART1_DSR have changed state and the four values are comma seperated.
Possible Responses	OK +CME ERROR: n

AT+FUP (Enter bootloader mode)

Command	**AT+FUP**
Description	Enter bootloader mode. **Note:** There should be no whitespace after *P* other than the terminating carriage return.
Possible Responses	OK +CME ERROR: n

AT+GCTM (Query GATT Table Schema of BLE peripheral)

Command **AT+GCTM hIdx**

Description

This is a GATT client-related command.

Use it to obtain the GATT table schema (such as the structure) of the peer connected on the handle identified by hIDx.

This results in many responses starting with either *TM:S* or *TM: C* and *TM: D*.

For example, the following from a device contains three services:

- First service – Contains four characteristics
- Second service – Contains one characteristic
- Third service – Contains four characteristics

In addition, the characteristic in the second service has a descriptor. In total, there are three descriptors in the entire GATT table.

```
AT+GCTM1
TM:S:1 ,(9) ,FE011800
TM: C:3 ,00000002 ,FE012A00 ,0
TM: C:5 ,00000002 ,FE012A01 ,0
TM: C:7 ,00000002 ,FE012A04 ,0
TM: C:9 ,00000002 ,FE012AA6 ,0
TM:S:10 ,(13) ,FE011801
TM: C:12 ,00000020 ,FE012A05 ,0
TM:  D:13 ,FE012902
TM:S:14 ,(65535) ,FD021101
TM: C:16 ,00000010 ,FD022000 ,0
TM:  D:17 ,FE012902
TM: C:19 ,0000000C ,FD022001 ,0
TM: C:21 ,00000010 ,FD022002 ,0
TM:  D:22 ,FE012902
TM: C:24 ,0000000C ,FD022003 ,0
OK
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Where:

TM:S	Indicates the start of a BLE service whose starting attribute handle is the integer value after the second '**:**' in that line.
The next integer parameter (in brackets)	The last attribute handle in that service.
Last eight-digit hex number	The UUID handle supplied by the firmware ***Note:*** *This is not the index mentioned in the AT+UUID command description.*

TM: C	Indicates the start of a BLE characteristic
The integer after the second ':'	The handle for the value attribute
The next integer	Eight-digit hex value that denotes the characteristic properties (see command AT+GSCB for details)
The next eight-digit hex number	The UUID handle supplied by the firmware
The final decimal number	Is always 0. Intended as a place holder for the *Included Service UUID Handle*. ***Note:*** *We have not yet encountered an Included Service. We will add this functionality as needed.*

TM: D	Indicates the start of a BLE descriptor that belongs to a characteristic (such as CCCD)
The integer after the second colon (:)	Its attribute handle
Next hex number	The UUID handle supplied by the firmware. The last four digits of the UUID are the 16-bit adopted UUID if the first four digits are FE01. For example, if the last four digits are 2902, it is a CCCD. This means that you can use the attribute handle with the AT+GCWC command to write an enable/disable notify/indicates for the characteristic to which it belongs.
The host processing the TM responses know there are no more to come when it receives either an OK or ERROR message.	

Possible Responses

```
OK
+CME ERROR: n
TM:S
TM: C
TM:  D
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+GCFA (Query Handle for Service/Char combination of BLE peripheral)

Command **AT+GCFA hIdx, uS, x, uC, y <,uD,z>**

Description

This is a GATT client-related command.

Use this command to search for the handle of the value attibute of a characteristic or the attribute handle of a descriptor attached to a characteristic in the peer connected on the handle identified by hIDx.

<uD,z>	(Optional) When this is absent, it implies that the search is for the value handle of a characteristic. When present, it implies that the search is for the descriptor. `OK` or `ERROR` terminates this command. If a characteristic or descriptor is found, the FC or FD responses have been received respectively.
uS uC uD	These are the UUID index that were used to pre-create a UUID handle using the command AT+UUID.
x y z	The 0-based instance index of the appropriate entity in the remote GATT table. For example, if x=1, y=2, and z=0, it means search for the second instance of a service with the UUID *uS*. In that service, search for the third instance of the characteristic with UUID *uC*; and in that characteristic, look for the first instance of the descriptor with UUID *uD*. **Note:** Typically, GATT tables do not have multiple instance services.

The main use of such a command is to locate a characteristic or descriptor in a server device to obtain the attribute handle so that it can be subsequently used in read/write requests using commands AT+GCRD, AT+GDWA, AT+GCWC.

This command immediately responds with OK or ERROR and, at some time subsequent, the asynchronous response FC or FD is received

When the attribute handle specified in the FC or FD is 0, it implies that the object was not found in the remote GATT table.

Possible Responses

```
OK
+CME ERROR: n
FC
FD
```

AT+GCRD (Read remote GATT attribute value by handle)

Command **AT+GCRD hIdx, hAttr, nOffset**

Description

This is a GATT client-related command.

It is used to read the content of a remote attribute starting at offset specified within that attribute. For example, if the attribute contains *Hello World,* setting nOffset to 6 results in *World* being read.

hIdx	The connection handle of the server from which it reads
hAttr	The attribute of the handle that was extracted using either AT+GCTM or AT+GCFA commands

This command immediately responds with OK or ERROR and at some time subsequent, the asynchronous response AR is received.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

If the read was successful then an AR response is received which contains the data. If the read failed (for example, if the attribute does not exist or it requires the connection to be authenticated), then the AS response is received. In rare occasions, an AB could also be received if, for example, the module is low in memory.

Possible Responses

```
OK
+CME ERROR: n
AR
AS
AB
```

AT+GCWA (Write remote GATT attribute value by handle, expect ACK)

Command

AT+GCWA hIdx, hAttr, hexdatastring

Description

This is a GATT client-related command.

It is used to write data to an attribute in a remote GATT table and expects an acknowledgement which will be received as an asynchronous response AW after the terminating OK response.

hIdx	The connection handle of the server from which it reads
hAttr	The attribute of the handle that was extracted using either AT+GCTM or AT+GCFA commands
hexdatastring	A string consisting of only hexadecimal characters which must be an even number in length. It is converted to binary before writing to the peer.

It always writes to offset 0 in the destination attribute.

If the attribute rejects the write because say the connection is not encrypted, then the AW will have the appropriate status value.

Possible Responses

```
OK
+CME ERROR: n
AW
```

AT+GCWC (Write remote GATT attribute value by handle, no ACK)

Command

AT+GCWC hIdx, hAttr, hexdatastring

Description

This is a GATT client-related command.

It is used to write data to an attribute in a remote GATT table; it does not expect an acknowledgement after the terminating OK response. If the command fails to write the value then there is eventually a disconnection because the link supervision timer timeouts.

hIdx	The connection handle of the server from which it reads
hAttr	The attribute of the handle that was extracted using either AT+GCTM or AT+GCFA commands
hexdatastring	A string consisting of only hexadecimal characters which must be an even number in length. It is converted to binary before writing to the peer.

It always writes to offset 0 in the destination attribute.

If the attribute rejects the write because the connection is not encrypted, for example, then the AW has the appropriate status value.

Possible Responses

```
OK
+CME ERROR: n
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+GSMD, AT+GSCB, AT+GSCE, AT+GSSB, AT+GSSE (Populate local GATT table)

Command

AT+GSMD m, rdRights, wrRights, len

AT+GSCB uC, prop, mVal <,mCccd<,mSccd>>

AT+GSCE hexdatastring

AT+GSSB uS

AT+GSSE

Description

These are GATT server-related commands used to populate the local GATT server table with services, characteristics, and descriptors.

A characteristic can have properties like read/write and CCCD and/or SCCD descriptors which may or may not require authentication.

When adding a characteristic, those attributes must be specified. You can achieve this by using a metadata object which must be pre-created using the AT+GSMD command. Just like UUID handles management, this app provides for an array of metadata objects that are referenced using the index *m* in the range 0 to 3.

AT+GSMD is used to create a metadata object in array index *m* and creates an opaque integer value that contains the read and write which can be any one of these values:

0	No access
1	Open
2	Encrypted with no man-in-the-middle (MITM) protection
3	Encrypted with man-in-the-middle (MITM) protection

Once the metadata object is created its index can be used to refer to in any command (like AT+GSCB) that needs it.

AT+GSSB	Used to define the start of a service which has a UUID that was pre-created using the AT+UUID command
AT+GSSE	Used to define the end of a service so that a new service can be added using AT+GSSB.
AT+GSCB	Used to define a characteristic which can have a CCCD and/or SCCD descriptors attached to it. If the arguments mCccd and mSccd are not supplied then the characteristic has neither. To add a SCCD but not a CCCD, use the syntax **,,mScc** where the empty field between the two commands conveys that desire. The parameter *uC* is the index of a UUID handle was pre-created using AT+UUID; and *prop* is a bit mask whose value is in the range 1 to 63 (0x3F) which are the properties as per the definition in the Bluetooth Specification. The following are the properties:

0	Broadcast-capable (Sccd descriptor must be present)
1	Can be read by the client
2	Can be written by the client without an ACK
3	Can be written (ACK is sent back)
4	Can be notifiable (Cccd descriptor must be present)
5	Can be indicatable (Cccd descriptor must be present)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+GSCE	Used to commit the new characteristic and *hexdatastring* supplies the initial value (after conversion to binary). If CCCD or SCCD descriptors are specified, then the initial values are 0. This command responds with an integer value in the *\nNN\r* format (an integer value in the range 0 to N). This integer value is an index value into an array of handles which MUST be noted by the host as associated with the newly created characteristic which is referenced in the commands AT+GSWC, AT+GSNO, and AT+GSIC. Think of this index value as an identifier.

Possible Responses

```
OK
+CME ERROR: n
```

AT+GSIC (Send Characteristic value Indication, ACK expected)

Command **AT+GSIC i,hexdatastring**

Description

This is a GATT server-related command and is used to send a value indication if the client has enabled indications via the referenced characteristic's CCCD.

i	The characteristic identifier that was returned by the AT+GSCE command
hexdatastring	The data that is first converted to binary and is then sent as an indication to all clients that enabled them.

When the indication is acked by the client, it results in an asynchronous AK message.

Possible Responses

```
OK
+CME ERROR: n
AK
```

AT+GSNO (Send Characteristic value Notification, ACK not expected)

Command **AT+GSNO i,hexdatastring**

Description

This is a GATT server-related command and is used to send a value notification if the client has enabled notifications via the referenced characteristic's CCCD.

i	The characteristic identifier that was returned by the AT+GSCE command
hexdatastring	The data that is first converted to binary and is then sent as an indication to all clients that enabled them.

Possible Responses

```
OK
+CME ERROR: n
```

AT+GSWC (Overwrite new value in local characteristic)

Command AT+GSWC i,hexdatastring

Description

This is a GATT server-related command and is used to set a new value for the characteristic indentified by *i*. If the characteristic was created with a property bit set for readable, then a remote GATT client is able to read this new value when it next polls it.

i refers to the characteristic identifier that was returned by the AT+GSCE command. *hexdatastring* is the data that is first converted to binary and then sent as an identification to ALL the clients that have enabled them.

Possible Responses

```
OK
+CME ERROR: n
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+LADV (Start NonVsp adverts)

Command `AT+LADV <advType <,advIntvlMs>>`

Description Start adverts which are non-vSP related. If the optional parameters are missing, then default values are used. S register 108 is used for the advType and S register 208 for advIntvlMs. Please note that these default values are cached on powerup/reset and so, if the S registers are changed, there must be an AT&W and then a reset.

If this command is received when in VSP mode, it exits to non-VSP mode and remains in that new mode.

Possible Responses

```
OK
+CME ERROR: n
```

AT+LADVX (Stop all adverts)

Command `AT+LADVX`

Description Stop all adverts.

Note: If an incoming connection is established, then adverts are automatically stopped and a new AT+LADV command is required to restart adverts.

At anytime, use the command Ati2016 to determine the current status of advertising. Bit 0 is set if the module is advertising.

Possible Responses

```
OK
+CME ERROR: n
```

AT+LCON (Initiate a NonVsp connection)

Command `AT+LCON address`

Description Make a non-vSP connection, with a slave latency of 0, to the device identified by *address* which is a 14-digit hex string (such as 000016A40B1623). To make a VSP connection, use command ATD.

On connection, the *connect* response contains parameters as detailed in the next chapter chapter describing all responses, but it is important to state here that, given there can be multiple non-vsp connections, they must be identified. A number between 1 and N is provided in that response so that it can be subsequently used to interact with the device on that connection.

Note: Handle is 1 and above. 0 is used internally for special use to identify the one VSP connection that is possible.

It uses the following S reg values to expedite the connection:

300	Minimum connection interval
301	Maximum connection interval
206	Link supervision timeout
110	Connection timeout (wait this long for peer to accept)

To change these values prior to initiating a connection use the command ATSxxx=yyyy which is also described in this guide.

The slave latency is negotiated by the peripheral device when there is a renegotiation attempt five seconds into the connection.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Then the AT parser is suspended until either a *connect*, *discon,* or an *ERROR* response is sent.

For example, if the address specified is not exactly a 14-digit hexstring then the *ERROR* response is sent.

Possible Responses

```
connect…
discon
+CME ERROR: n
```

AT+LMTU (Negotiate ATT MTU for NonVsp connection)

Command

```
AT+LMTU hIdx
```

Description

Use this command when in non-VSP mode to trigger a MTU request where the att size is as per the #define DLE_ATTRIBUTE_SIZE in the AT interface application.

Expect MT asynchronous messages descibed in the responses section below if an OK is returned.

Possible Responses

```
OK
+CME ERROR: n
```

AT+LPHY (Change PHY for NonVsp connection)

Command

```
AT+LPHY hIdx
```

Description

Use this command when in non-VSP mode to trigger a PHY change request as per Sreg 100.

Expect PU or PF asynchronous messages descibed in the responses section below if an OK is returned. PU is when the PHY is successfully changed.

Possible Responses

```
OK
+CME ERROR: n
```

AT+LDSC (Disconnect a NonVsp connection)

Command

```
AT+LDSC hIdx
```

Description

Use this command when in non-VSP mode to drop a connection which is identified by the integer *hIdx*, that was supplied in the *connect* response. It is a value in the range 1 to N and initiates a disconnection and sometime later after an OK response is sent the actual disconnection occurs and at that time the *discon* message is sent.

Possible Responses

```
OK
+CME ERROR: n
```

AT+LENC (Request encryption on NonVsp connection)

Command

```
AT+LENC hIdx
```

Description

Use this command when in non-VSP mode to encrypt a connection which is identified by the integer *hIdx*, that was supplied in the *connect* response. It is a value in the range 1 to N and initiates the negotiation with the peer for the connection to go encrypted and sometime later after an OK response is sent, the *encrypt hIdx* message is sent.

Possible Responses

```
OK
encrypt hIdx
+CME ERROR: n
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+LSCN (Start scanning for adverts)

Command	`AT+LSCN <timeout_sec <,"escaped_pattern"<,rssi>>>`
Description	Start **scanning** for adverts. All parameters are optional and, if missing, the default value for timeout is obtained from S register 106, and *escaped_pattern* is set to an empty string and RSSI is set to -128. If *escaped_pattern* is specified, then it could be something like **Hello\20World\0D** which ends as a 12-byte string. Advert responses are only sent to the host if it contains a match **anywhere** in the string. If the rssi value is also specified, then the response is sent if the RSSI value of that advert is equal or greater in value. This allows the host to ignore devices that are further away. If the *escaped_pattern* string is empty and RSSI value is specified then this is a filter that allows all adverts that have an RSSI greater than or equal to that specified. This filter mechanism also allows only adverts with certain advertised services to be pushed to the host. If, in VSP mode of operation and the timeout_sec is set to 0, then it exits from VSP operation mode into non-VSP mode and stays in that mode. Otherwise, the AT parser is suspended for the timeout value specified while scanning is in progress.

Possible Responses	`OK`
	`+CME ERROR: n`
	`AD0:...`
	`AD1:...`

AT+LSCNX (Stop scanning for adverts)

Command	`AT+LSCNX`
Description	Stop scanning.
Possible Responses	`OK` `+CME ERROR: n`

AT+LVSP (Enable VSP mode of operation)

Command	`AT+LVSP`
Description	When in non-vSP mode, this command sets the module into vSP mode. This means if the vSP service is not already installed in the GATT table, it is installed.
Possible Responses	`OK` `+CME ERROR: n`

AT+PAIR (Initiate pairing on NonVsp connection)

Command	`AT+PAIR hIdx`
Description	Use this command when in non-VSP mode to initiate a pairing with the device on the connection identified by the index handle hIdx. Some time later, if OK was sent and if pairing is successful, the asynchronous response *encrypt* is sent and, if the pairing I/O capability S register 107 is not JustWorks, there is other intervening responses related to authentication which require a response, such as: ▪ dispcode ▪ passkey? ▪ oobkey? ▪ xxkey?

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

The response commands to these asynchronous responses are detailed in the later section related to responses. As this is all event driven using responses, it is sufficient to just act accordingly when the events happen as detailed.

At any time the command ATI2009 returns the number of devices in the trusted device database.

In VSP mode, if via S register 102 an encrypted VSP connection is enforced and S107 is set to 0 (i.e JustWorks) and the device is not trusted, then it allows a pairing during the connection initiated by ATD.

Possible Responses

```
OK
+CME ERROR: n
```

AT+PRSP (While pairing provide passkey/code/oobkey when challenged)

Command

```
AT+PRSP hIdx,[Y|y|N|n]
AT+PRSP hIdx,32HexDigitNumber
AT+PRSP hIdx,nnn
```

Description

If pairing I/O capability was appropriately set via S register 107 so that this module has a user-interface to expedite an authenticated pairing (as opposed to Just Works), then during the pairing process (which is initiated by the AT+PAIR command), if the peer device also has pairing capability, then the variant of this command to use is as per the response as follows:

- dispcode :: AT+PRSP hIdx,[Y|y|N|n]
- passkey? :: AT+PRSP hIdx,nnn
- oobkey? :: AT+PRSP hIdx,32HexDigitNumber
- xxkey? :: AT+LDSC hIdx

hIdx	Same value a per supplied in the response from the module
[Y|y|N|n]	One of the four single characters to imply a Yes or No
nnn	An integer value in the range 0 to 999999
32HexDigitNumber	A hexadecimal string consisting of exactly 32 characters

If *xxkey?* is received which is unexpected, then the best action is to disconnect and exists to future proof the device just in case a future Bluetooth specification adds a new type of pairing authentication mechanism.

Possible Responses

```
OK
+CME ERROR: n
```

AT+SFMT (Set display format of incomming scanned adverts)

Command

```
AT+SFMT <frmt>
```

Description

<frmt> can take the range 0..1
When AT+LSCN is used to scan for adverts it will display each advert in a default format where only the device name from the advert data is displayed. That default format is specified by frmt=0 and will be the default value if <fr,t> value is not provided.
If frmt=1 then the full advert/scan report data is displayed in hex format.

Please note that user is free an d encouraged to add more formats

Possible Responses

```
OK
+CME ERROR: n
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+SIOC (Configure functionality of a gpio pin)

Command	`AT+SIOC sionum,func,subfunc`
Description	The module has many digital and analog I/I pins. They are referred to as Signal Input/Output (SIO for short) pins. They are configurable to be digital or analog and can be in or out and some can even have special functions like PWM (pulse width modulation) or even frequency output. Individual pins are configured using this command. *Sionum* is a value in the range 1 to N which identifies the signal pin number *Func* is as follows: ▪ 1 – Digital_IN ▪ 2 – Digital_OUT ▪ 3 – ANALOG_IN. Subfunc are values that further qualify the Func value. Refer to the user guide of the module for more details – locate the description of the function GPIOSETFUNC() .
Possible Responses	`OK` `+CME ERROR: n`

AT+SIOR (Read gpio input value)

Command	`AT+SIOR sionum`
Description	Once a signal pin is configured using the AT+SIOC command, if it was configured as a digital_in or analog_in, this command retrieves the current value which is 0 or 1 for digital and a value 0 to N for analog. The integer value returned has a starting \n character and a \r ending character.
Possible Responses	`OK` `+CME ERROR: n`

AT+SIOW (Write value to gpio output)

Command	`AT+SIOW sionum,val`
Description	Once a signal pin is configured using the AT+SIOC command, if it was configured as a digital_out, this command sets the current value which is 0 or 1.
Possible Responses	`OK` `+CME ERROR: n`

AT+URTC (Config baud+flow of 840 main uart connected to host)

Command	**`AT+URTC baud,flow`**
Description	Close and re-open the main port with the baud rate and optional CTS/RTS flow control specified. 'flow' is 0 for none and 1 for CTS/RTS flow control. It is valid to have the auxiliary and main UART port to be at different baud rates. To non-persistently change operation of the auxiliary port use the command AT+AUXC. Please note the response will be sent at the new baud rate and so if the host has not matched that baud rate within 2000 milliseconds, then it will be seen as garbage. The delay is implemented using a spin function and so for that 2000ms the application will not service any events.
Possible Responses	`OK` `+CME ERROR: n`

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+UUID (Create a UUID handle)

Command

```
AT+UUID u,16bitUuid
AT+UUID u,32HexDigitNumber
AT+UUID u,16bitUuid,v
```

Description

BLE makes wide use of UUIDs (universally unique identifiers) which are 128-bit (16-byte) random values. These values can be cumbersome to manage as string objects. Because of this, the module firmware exposes a concept of a 32-bit integer value which is a handle to an internal 16-byte buffer that contains the actual value.

The *smart*BASIC application exposing the AT interface functionality extends that concept by using an array of integer variables to store those handles provided by the firmware. Those firmware handles are never exposed, but instead an index value *u* is.

The *u* in these three variants of the command is the index into that integer array. Consider a bunch of mailboxes numbered 0 to N (see MAX_UUID_HANDLES in the source code) which are your scratchpads to load UUID handles into (using these commands) as and when you need to supply a UUID into any of the AT commands that require a UUID.

For example, the command AT+GSSB takes a parameter which is one of these 0 to N indices.

The value for *u* shall always be in the range 0 to N, where N is 15 at the time of writing and can be modified by changing the #define for MAX_UUID_HANDLES.

The command variant AT+UUID u,16bitUuid is used to create a handle from a Bluetooth SIG adopted 16-bit UUID and store it in the array index *u*. The value 16bitUuid shall be in the range 0 to 0xFFFF.

The command variant AT+UUID u,32HexDigitNumber takes the 32-character hexadecimal string and converts that into a handle and stores it in the array index *u.*

The command variant AT+UUIS u,16bitUuid,v takes the 16bitUuid which is a value in the range 0 to 0xFFFF and creates a sibling of the handle stored in array index v and stores in array index *u*. By sibling, it is meant that the base UUID of the handle stored in array index *v* is used to create the new UUID.

Possible Responses

```
OK
+CME ERROR: n
```

ATD (Initiate a streaming VSP connection)

Command

```
ATD address
```

Description

Make a VSP connection, with a slave latency of 0, to the device identified by address which is a 14-digit hex string (for example, 000016A40B1623). To make a non-VSP connection, use command AT+LCON.

Note: When an incoming or outgoing connection is established, the VSP stream is bridged directly to the HL78 not to the Host on the main UART.

*** If in mux mode 0 (S Register 120 is 0) then an outgoing connection is disallowed. ***

It uses the following S register values to expedite the connection:

- 300 – Minimum connection interval
- 301 – Maximum connection interval
- 206 – Link supervision timeout
- 110 – Connection timeout (wait this long for peer to accept)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

To change these values prior to initiating a connection, use the command ATSxxx=yyyy which is also described in this guide.

After this command is processed, the AT parser is suspended until either a CONNECT or a NOCARRIER response is sent. Please note this is one of the few commands that is NOT terminated by an OK or ERROR response.

If the address specified is not exactly a 14-digit hex string then the NOCARRIER response is sent.

On a successful connection, the bi-directional on-air stream is bridged to the auxiliary UART interface which is connected to the cellular modem chipset. AT commands sent from the BLE peer are processed by the cellular chipset and its response is sent back over the air.

Possible Responses

```
CONNECT…
NOCARRIER nn
```

ATH (Disconnect a VSP connection)

Command **`ATH`**

Description If there is an ongoing VSP connection, then this will be dropped. Regardless of whether there is a connection or not, an OK response will be sent. There will eventually be an asychronous “NO CARRIER” response.

Possible Responses `OK`

ATI (Get Information)

Command `ATI n`

Description Get read-only information identified by integer n. A value is returned that could be an integer or a string that starts with a \n and ends with a \r.

The following information is returned with identifier ‘n’ as stated (refer to user guide for the module for more n values in the section related to the function SYSINFO):-

Reg	Description
0	The value of #define AT_RESPONSE_0 in the source code E.g: PINNACLE 100
3	The firmware version of the module (see n=23 for version of app)
4	The MAC address of the module as a 14-digit hex string
10	The value of #define AT_RESPONSE_10 in the source code. E.g: Laird,(c)2017
23	The version of the *smart*BASIC application, which is the value of #define LibVer
33	The version of the *smart*BASIC application, which is the value of #define AppVer and can be changed by the customer in top level .sb file
42	The value of the current state of a state machine implemented by the app
50	Count of NFC Coil energize/de-energize events. **Will be an odd number if the coil is still energized.** When this count is read, all bits except bit 0 are reset. Wraps to 0 after 2^31
51	Count of the number of times the NFC tag is read. When this count is read, it is reset Wraps to 0 after 2^31
2009	Number of devices in the trusted device database
2012	Maximum number of devices that can be saved in the trusted device database

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Possible Responses

```
OK
+CME ERROR: n
```

ATS (Read/Write/Query Numberic Registers)

Command

```
ATS n=m
ATS n?
ATS n=?
```

Description

These commands are to set and get values, as well as the range of valid values, for any S register (respectively) where the S register is identified by the integer value n. When setting, *m* is the new value.

For the *n?* and *n=?* variants, the returned value is enclosed in \n and \r and is sent before the OK. The max and min integer values returned by *n=?* are separated by a comma.

Note: When setting the value, it is not retained over a power cycle or a warm reset triggered using the ATZ command. See the AT&W command to make all changed values permanent.

The following S Registers are defined:

Register	Description
100	*Startup Flags* ▪ Bit 0 – Set to VspConnectable - hence populates GATT table and starts adverts ▪ Bit 1 – Ignored if bit0 is 1 otherwise start advertising with no timeout ▪ Bit 2 – Ignored if bit0 is 1 otherwise start scanning with no timeout ▪ Bit 3 – Set for max bi-directional throughput of about 127 kbps, otherwise half that. ▪ Bit 4 – Use Data Length Extension (#define DLE_ATTRIBUTE_SIZE) in *smart*BASIC application ▪ Bit 65 – Phy Rate 00 – 1MPHY 01 – Long Range – 125 kbps 10 – RFU : will set 1 MPHY 11 – 2MPHY
101	*TxPower_dBm* Valid values are 8,7,6,5,4,3,2,0,-4,-8,-12,-16,-20,-40
102	*Encryption Requirement for incoming VSP connections* ▪ Bit 0: Enable(1)/Disable(0) ▪ Bit 1: (MITM(1) /NoMITM(0)
103	*Device Name Format in adverts and Gap Service (valid values 0 to 7)* If this value is 0, then the name is DEVNAME. This is specified using the string S Register command AT%Sn=s where n is 0 and the command AT%S is described elsewhere in this section. If this value is non-zero, then the name is DEVNAME-HH..HH where the number of HH is exactly double the value in this register and those hex digits correspond to the rightmost hex characters of the MAC address. For example, if the MAC address is 0123456789ABCD and this register contains 3, and the device name is ROCKS and the advertised device name is ROCKS-89ABCD. Also note that if the combined string is greater than the value set for

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

	#define MaxDevNameSize in the *smart*BASIC source code (which you are free to modify) then the name is the rightmost that many characters.
104	This is the slave latency that is negotiated when connected as a slave. This negotiation starts about five seconds after the connection is made.
105	*FlagsAD* This is the flags bit in the Flags AD element when adverts are started. It specifies general or limited discoverability. If not sure, use default value.
106	*Scan Timeout in seconds* When starting scans for adverts using the AT+LSCN command, if the timeout value is omitted then the value in this register is used.
107	*I/O Capability to use during the initial negotiation when pairing.* This specifies the user interface that is available to expedite a pairing. Just Works pairing implies there is no user interface and so the resulting encryption key is not authenticated and so not immune to MITM (man-in-the-middle) attack. The following are valid values: ▪ 0 – Just Works ▪ 1 – Disp with Y/N ▪ 2 – Kboard only ▪ 3 – Disp Only ▪ 4 – Kboard+Disp
108	*Idle Advert Type* This specifies the advert type to use advertising in non-VSP mode. ▪ 0 – ADV_IND (Connectable and responds to scan requests) ▪ 1 – ADV_DIRECT_IND (Connectable but only from specific device) ▪ 2 – ADV_SCAN_IND (Not connectable, but responds to scan req's) ▪ 3 – ADV_NONCONN_IND (Not connectable, ignores scan req's) If this is changed, then a save using AT&W is required and only takes effect after the next power cycle or warm reset.
109	*Pin to use to control low power UART operation.* For low power UART operation, this GPIO line is monitored and, when low, the module is allowed to automatically close the UART after an idle period that is set via SRegister 213. Setting the value
110	*Connection Timeout in seconds* When making an outgoing connection using the command ATD or AT+LCON, this Sreg specifies the maximum time for connectable adverts from the device to be connected to.
111	*Reserved for future use*
112	*Active or Passive Scan Type* Set to 0 for passive scanning and 1 for active. Active scanning means that, if an advert is received with type ADV_IND or ADV_SCAN_IND, it sends a scan request so that the advertiser sends a scan response which contains a further 31 bytes made of AD elements. By default, this is set for active scanning.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

113	*Scan RSSI minimum in dBm* When scanning for adverts, each incoming advert is reported with the RSSI at which it was received. If the RSSI of that advert is less than specified by this S reg, then it is not reported to the host connected at the UART. This allows the host to filter adverts based on how weak the signal is (that is how far away it usually is). The default setting is -120 and so, given that the receive sensitivity is around -100, this implies that all adverts no matter how weak, if received, are reported to the host.
114	*Link Supervision Timeout (Seconds) as Slave* This is the link supervision timeout that is requested for an incoming connection after five seconds if the connection interval is not in the required range. This value is written to the GAP service on power up.
115	*Minimum Encryption Key Length* This can be between 7 and 16. Essentially at pairing, this information is determined and saved in the trusted device database. In the future, if a service requires a minimum key length for data exchange and the connection is encrypted and if the length of the key for that encryption is less that this value, data exchange cannot happen.
116	*MITM (man-in-the-middle) for Encryption Required* This is used by a central role device when it wishes to start encryption. If this set to 1, it implies that the encryption request shall only succeed if the stored key is authenticated when the most recent pairing happened. Valid values are 0 for no MITM requirement and 1 for required.
117	*TxPower_dBm while a connection is negotiating a pairing.* Valid values are 8,7,6,5,4,3,2,0,-4,-8,-12,-16,-20,-40 This improves security as setting a very low value requires the pairing peer to be very close as thus minimise sniff attempts
118	*Reserved for future use*
119	*Reserved for future use*
120	*UART Multiplexer mode* As per Figure 1 (in the *UART Multiplexer Modes* section) which shows a block diagram of the module, there is an application microcontroller with two UART ports that sits between the cellular module and the host. The MCU must bridge AT commands to that cellular modem to achieve data exchange over the cellular network. There MCU also has an AT command processor and so it can also process AT commands to expose BLE, NFC, and other functionality. There are three ways the host UART can be bridged to the cellular modem (referred to as multiplexer modes 0, 1, and 2 which are the values that can be set in this register). Mode 0 — The GPIO pin specified by SRegister 121 is used as an input to allow the host to control the destination of UART traffic. If it is high, all traffic is relayed to and from the cellular modem and, if low, the traffic is processed by the application microcontroller. Mode 1 — The default mode that, along with SRegister 122, specifies the initial startup state. Traffic is either directed to the cellular modem or

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

		the application processor. When SRegister 122 is 1, then on startup traffic goes to the cellular modem and if 0 it goes to the application processor. If you send the command ATI0, the response is *PINNACLE 100* if traffic is directed to the application processor and is *HL7800* if directed to the cellular modem. If traffic is currently going to the application processor, the traffic can be toggled to the cellular modem by sending the AT! command. If traffic is currently going to the cellular modem, traffic can be toggled back to the application processor by sending the ! ! ! escape sequence.
	Mode 2	An intelligent operation mode which is slower because the traffic is always monitored by the application processor. All commands starting with lower case ***at*** is forwarded to the cellular modem. The logical switch remains in that direction until there is an OK or an ERROR which terminates that transaction. All commands starting with upper case ***AT*** are processed by the application processor. If it is not recognized, it is automatically relayed to the cellular modem and the logical switch remains in that direction until there is an OK or ERROR from the cellular modem. At any time, if there is no AT command transaction ongoing and the cellular modem has an asynchronous response to send, it is relayed to the host immediately. Otherwise, it waits for the AT transaction to complete with an OK or ERROR for that transaction to be relayed to the host.
121	*UART Multiplexer GPIO number*	If SRegister 120 specifies Mode 0 – This GPIO pin is configured as an input and is used by the host to control to where host UART traffic is directed. If 0 then traffic goes to the application processor; if 1 then it goes to the cellular modem. If SRegister 120 specifies Mode 1 – This GPIO is configured as an output to indicate to where host UART traffic is currently directed. It is low for application processor and high for traffic to the cellular modem.
122	*Multiplexer Mode 1 default direction*	Mode 1 – On power up, this specifies the default direction of the multiplexer. Set it to 0 to point to the nrf52840 microcontroller and to 1 to point to the HL7800. The default values is 1 so that any AT commands sent by the host are routed to the HL7800.
123	*UART Flow Control*	If set to 1 – This register specifies hardware CTS/RTS flow control is to be used for both UARTs on power up. If set to 0 – No handshaking for both UARTS. See S Register 302 for baud rate setting.
124	*Reset HL7800 on startup*	When the nrf52840 microcontroller is reset via pin M2.73, the *smart*BASIC application restarts. If this S Register is set to 1 then the HL7800 is reset. By default this register is set to 1

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

125 to 129	*Reserved for future use*
130 to 137	*Free to be used by the host to save non-volatile data* Valid values are -128 to +127
138 to 139	*Reserved for future use*
200	*VSP Encryption Disconnect Timeout (milliseconds)* If a VSP service is specified with encryption requirement, a timer is started on a VSP connection. If it times out before the connection is encrypted, the slave initiates a disconnection. This is a form of resilience to a denial-of-service attack, in which a device connects and then does nothing to prevent legitimate users from connecting. The timer is cancelled as soon as the connection goes encrypted.
201	*vSP Advert Interval (milliseconds)* When starting adverts for incoming VSP connections, this specifies the advert interval to use.
202	*Host UART Transmit Buffer Size*
203	*Host UART Receive Buffer Size* The size of the UART transmit and receive ring buffers. 0 means use default.
204	*VSP Transmit Buffer Size*
205	*VSP Receive Buffer Size* The size of the VSP transmit and receive ring buffers.
206	*Link Supervision Timeout in milliseconds* When making an outgoing connection using ATD or AT+LCON, this S reg specifies the link supervision timeout to use in the connection request.
207	*Appearance (Optionally used in Adverts)* Specifies the value to use in the Appearance AD element in an advert. A value of 0 implies that the Appearance AD element is not added to the advert report.
208	*Idle Advert Interval in milliseconds* When advertising in non-VSP mode, this specifies the default advert interval. Also used when not supplied in the AT+LADV command.
209	*GATT Client memory size* Use this to specify the memory the GATT client reserves for itself when it is opened for any GATT client activity. Only modify this if memory becomes tight due to many *smart*BASIC variables being declared. Adjustment of this S reg is rare.
210	Bitmask containing Extra Flags as follows: ▪ Bit 0 – If set, the Autorun pin is not relocated (use with care) ▪ Bit 1 – If set, VG/G2/G6/DS async responses are enabled when mux points to 840 and the VGPIO/GPIO2/GPIO6/UART1_DSR lines change state.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

- Bit 2 – If set, AX asyn response is enabled when mux points to 840 and there is new data from HL7800 saved in the auxilliary uart rx buffer.

  By default, all flags are set to 0.

211	*Scan Interval in milliseconds*
212	*Scan Window in milliseconds* When a scan for adverts in initiated, these registers specify the interval and window respectively, for scanning. The ratio of window over interval specifies the duty cycle. When both are set to the same value, the duty cycle is 100%, with minimal probability that an advert report is missed. However, setting 100% duty cycle implies the radio receiver is ON all the time. This results in maximum power consumption. Setting the ratio as low as possible reduces power consumption but at the expense of missing adverts.
213	*Host UART Idle Time in milliseconds for low power UART operation* When the low power version of this application is loaded into the module, if the module detects that there is no UART activity for this period of time AND the *keep UART open* input line is low (see S Register 109), then it automatically closes the UART. If there is incoming data over the air that needs to be conveyed to the host, then the UART is automatically opened regardless of the status of the *keep UART open* input line.
214	*Multiplexer Mode 1 escape delay in milliseconds* When SRegister 120 is 1 and host traffic is relayed to the cellular modem and the host wants to send AT commands to the application processor, the *!!!* escape sequence is used to toggle the host UART traffic routing. This register specifies the minimum delay that must be present either side of each *!* character.
215	*Auxillairy UART Transmit Buffer Size* The UART that services communications with the cellular modem
216	*Auxillairy UART Receive Buffer Size* The UART that services communications with the cellular modem
2xx	*Free to be used.* Currently *xx* is 13 to 19. Valid values: -32768 to +32767
300	*Minimum Connection Interval in microseconds*
301	*Maximum Connection Interval in microseconds* When making an outgoing connection using ATD or AT+LCON, these specify the minimum and maximum intervals that are acceptable for the connection interval. A range must be specified to give the stack flexibility in arranging the optimal connection intervals when there are multiple connections. If you are going to only have a VSP connection and so know that the radio is not going to 'object', it is possible to set both these values to the same value. In this case you should get the value you require. When the connection is established, it is reported using the CONNECT response which supplies the actual interval negotiated by the stack with the peer.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

	302	*UART Baud Rate* Specifies the baud rate to use for commands and data transfer. After setting, a power cycle or a warm reset is required.
	303	*VspTxUUID*
	304	*VspRxUUID*
	305	*VspMdmInUUID*
	306	*VspMdmOutUUID* Values in the range 0x0 to 0xFFFF; the 16-bit UUID offsets to use for the vSP service. Changing this means that mobile apps supplied by Laird to interact with vSP stop working as they do find the expected UUIDs. Only change this if absolutely necessary. A good reason to change it is to make the vSP private to you; other devices expecting the standard Laird UUID will not work. This is an additional way to restrict access to your device.
	3xx	*Free to be used.* Currently *xx* is 07 to 09. Valid values: -2147483648 to +2147483647
Possible Responses	`OK` `+CME ERROR: n`	

ATZ (Warm Reset 840 and Cold Reset HL7800)

Command	`ATZ`
Description	Restart the module by performing a warm reset.
Possible Responses	`OK`

3.5 Responses

To simplify reception of messages in the receiving device, each message starts with a \r\n character sequence and ends with the same \r\n character sequence. It may also contain additional embedded \n characters where \n is the linefeed character with ASCII code 0x0A and \r is the carriage return characters with ASCII code 0x0D.

After stripping the \r\n start sequence, each response starts with a unique two-character sequence to help the host decode the response quicker in a stateless manner.

Some responses are synchronous which mean they are used to terminate a command so that the command parser can process more commands.

3.5.1 Response: Synchronous and Terminating

When a host receives these responses it can issue new commands and expect them to be processed immediately.

`CONNECT 0,address,interval,sprvsnTout,latency`

The command ATD successfully created a VSP connection to the device with the MAC address where:

- *interval* is the connection interval is *interval* (in microseconds)
- *sprvsnTout* is the link supervision timeout (in microseconds)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

- *latency* is the slave latency

The first parameter is always *0* as that handle index is dedicated for VSP connections.

+CME ERROR: n

A command is not successfully actioned and *n* is an error code. Error codes are as follows:

01	Invalid S Reg number
02	Value supplied is out of range
05	Syntax error
09	Invalid Address was supplied
14	Command cannot be processed in current state
15	Unknown command
33	Supplied value is not valid
46	Specified GPIO is not available
47	Too few parameters supplied
48	Too many parameters supplied
49	Invalid hex string
50	Save fail
51	Restore fail
52	VSP open fail
53	Invalid advert type
54	Invalid UUID
55	Service not ended
56	Characteristic not ended
57	Service not started
58	Too many characteristics
59	Characteristic not started
60	NFC not open
61	NFC NDEF message empty
99	Functionality not coded
HHHH	Four hex digits are other codes that are raw *smart*BASIC resultcodes. Refer to UwTerminalX lookup for meaning.

NOCARRIER 0

The command ATD failed to establish a VSP connection.

OK

A command was successfully expedited.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.5.2 Response: Synchronous and Not Terminating

When a host receives these responses it cannot issue new commands and expects them to be processed immediately as a terminating response is still to come.

TM:S:i ,(j) , HHHHHHHH

AT+GCTM command in progress. This specifies details of an attribute in a remote table that contains a Service attribute.

- *i* – An integer number which is the attribute handle
- *j* – An integer number which is the last attribute handle in this service
- *HHHHHHHH* – An eight-digit hex value corresponding to a UUID handle. If the first four HHHH is *FE01*, then it is a Bluetooth SIG-adopted UUID and the 16-bit value is the next four digits.

TM: C:i ,000000PP , HHHHHHHH ,0

AT+GCTM command in progress. This specifies details of an attribute in a remote table that contains a Characteristic attribute.

- *i* – An integer number which is the attribute handle
- *HHHHHHHH* – An eight-digit hex value corresponding to a UUID handle. If the first four HHHH is *FE01*, then it is a Bluetooth SIG-adopted UUID and the 16-bit value is the next four digits.
- Final *0* – This is for future use and is related to included services.

Note the single space between the first **:** and the *C*.

TM: D:i ,HHHHHHHH

AT+GCTM command in progress and this specifies details of an attribute in a remote table that contains a Descriptor attribute.

- *i* – An integer number which is the attribute handle
- *HHHHHHHH* – An eight-digit hex value corresponding to a UUID handle. If the first four HHHH is *FE01*, then it is a Bluetooth SIG-adopted UUID and the 16-bit value is the next four digits.

Note the single space between the first **:** and the *D*.

ENCRYPT

The command ATD is in progress and has reached the encrypted state before final confirmation (which is the CONNECT response).

3.5.3 Response: Asynchronous

A host must be designed to expect any of these responses at any time. To help with enabling a host to be as stateless as possible, all these responses have a unique two-letter starting sequence to quickly determine what it means and how it gets processed.

AB:hIdx, respcode

Triggered when the AT+GCRD command attempts to read the content of an attribute in a remote GATT table – It is successful but fails to store that content locally. RespCode is a value referenced in the Laird utility UwTerminalX.

AD0:t addr14hex rssi "name"
AD1:t addr14hex rssi "name"

These messages occur asynchronously when scanning for adverts. The *AD1* variant is when scanning using the AT+LSCN command while waiting for an incoming vSP connection.

- *t* – The advert type. 0 to 3 as per the Bluetooth specification where *0* implies that the advert is connectable.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

- *addr14hex* – A hex string exactly 14-charaters long. It is the address present in the advert; the first two characters are used to determine the type (such as resolvable, static, etc.).
- *rssi* – The RSSI of the received packet. It is usually a value between about -30 and -100. The lower the number, the weaker the signal.
- *name* – The device name if it was supplied in the advert.

None of the other AD elements are displayed. Should the developer want that information to display, then it is encouraged that the supplied *smart*BASIC application be modified as required.

See function HndlrAdvReport00() which is called each time an advert report is received and look for the *print* statement.

AK:i

An indication initiated using the AT+GSIC command of acknowledgement.

- *i* – The index of the characteristic that was indicated.

To recap, *i* was provided when the characteristic was entered into the local GATT table using the AT+GSCE command.

AR:hIdx, offset, hexdatastring

Triggered when the AT+GCRD command is used to read the content of an attribute in a remote GATT table and it successfully reads it.

- *hIdx* – The connection handle index
- *offset* – The offset that was requested when the read was requested
- *hexdatastring* – The data in hex string format

AS:hIdx, erStatus

Triggered when the AT+GCRD command is used to read the content of an attribute in a remote GATT table and it fails.

- *hIdx* – The connection handle index
- *erStatus* – The reason for the failure. It is an integer value as follows:

Hex	Dec	Description
0x0001	1	Unknown or not applicable status
0x0100	256	Invalid error code
0x0101	257	Invalid attribute handle
0x0102	258	Read not permitted
0x0103	259	Write not permitted
0x0104	260	Used in ATT as Invalid PDU
0x0105	261	Authenticated link required
0x0106	262	Used in ATT as Request Not Supported
0x0107	263	Offset specified was pas the end of the attribute
0x0108	264	Used in ATT as Insufficient Authorisation
0x0109	265	Used in ATT as Prepare Queue Full
0x010A	266	Used in ATT as Attribute not found
0x010B	267	Attribute cannot be read or written using read/write blob requests
0x010C	268	Encryption key size used is insufficient
0x010D	269	Invalid value size
0x010E	270	Very unlikely error
0x010F	271	Encrypted link required
0x0110	272	Attribute type is not a supported grouping attribute

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Hex	Dec	Description
0x0111	273	Encrypted link required
0x0112	274	Reserved for Future Use – Range 1 Begin
0x017F	383	Reserved for Future Use – Range 1 End
0x0180	384	Application range begin
0x019F	415	Application range end
0x01A0	416	Reserved for Future Use – Range 2 Begin
0x01DF	479	Reserved for Future Use – Range 2 End
0x01E0	480	Reserved for Future Use – Range 3 Begin
0x01FC	508	Reserved for Future Use – Range 3 End
0x01FD	509	Profile and Service Error: (CCCD) improperly configured
0x01EE	510	Profile and Service Error: Procedure Already in Progress
0x01FF	511	Profile and Service Error: Out of Range

AW:hIdx, status

Triggered when the AT+GCWA command is used to write the content of an attribute in a remote GATT table and demonstrates the outcome of that attempt.

- *hIdx* – The connection handle index
- *status* – The integer value which is *0* for success (otherwise, a value as listed in the section for the *AS* response)

CC:i, newValue

This message happens asynchronously when a remote GATT client writes into a CCCD descriptor of one of the local characteristics identified by *i*, which was provided as a result of AT+GSCE when the characteristic was created and commited. The parameter *newValue* is an integer.

See responses *WR* and *SC* when the characteristic value and Sccd are written.

CM:s

This message happens asynchronously when the state of the HL7800 changes state. It will be a value between 0 and 4:

0	The HL7800 is coming out of reset and will not respond to AT commands.
1	RUN state
2	SLEEP state
3	LITE_HIBERNATE state
4	HIBERNATE state

VG:a

If enabled via Sreg210 bit 1 being set and the multiplexer is pointing to the 840, this message happens asynchronously when the state of the HL7800 output line VGPIO changes, where *a* is 0 or 1 and signifies the new state of that line.

Note: By default, this response is not sent and can be enabled using Sregister 210 which is a bitmask.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

G2:a

If enabled via Sreg210 bit 1 being set and the multiplexer is pointing to the 840, this message occurs asynchronously when the state of the HL7800 output line GPIO2 changes, where *a* is 0 or 1 and signifies the new state of that line.

Note: By default this response is not sent and can be enabled using Sregister 210 which is a bitmask.

G6:a

If enabled via Sreg210 bit 1 being set and the multiplexer is pointing to the 840, this message happens asynchronously when the state of the HL7800 output line GPIO6 changes, where *a* is 0 or 1 and signifies the new state of that line.

Note: By default, this response is not sent and can be enabled using Sregister 210 which is a bitmask.

DS:a

If enabled via Sreg210 bit 1 being set and the multiplexer is pointing to the 840, this message happens asynchronously when the state of the HL7800 output line UART1_DSR changes, where *a* is 0 or 1 and signifies the new state of that line.

Note: By default, this response is not sent and can be enabled using Sregister 210 which is a bitmask.

AX:

If enabled via Sreg210 bit 2 being set and the multiplexer is pointing to the 840, this message occurs asynchronously when multiplexer is in mode 0 or 1 and it is pointing to the 840. It signifies that data was received from HL7800 and so flipping the multiplexer results in the data being sent to the host.

Note: By default this response is not sent and can be enabled using Sregister 210 which is a bitmask and the Sregister 120 contains the current multiplexer mode.

CONNECT 0,address,interval,sprvsnTout,latency

For a device waiting for an incoming VSP connection, this is an asynchronous message to confirm that a connection is fully setup from a device with MAC address where:

- *interval* – Connection interval in microseconds
- *sprvsnTout* – The link supervision timeout in microseconds
- *latency* – The slave latency

The first parameter is always *0* as that handle index is dedicated for VSP connections.

Note: A lower-case *connect* implies a non-VSP connection.

connect hIdx,address,interval,sprvsnTout,latency

For a device waiting for an incoming non-VSP connection, this is an asynchronous message to confirm that a connection is setup from a device with MAC address where:

- *interval* – Connection interval in microseconds
- *sprvsnTout* – The link supervision timeout in microseconds
- *latency* – The slave latency

The first parameter *hIdx* is the handle index which are non-zero and dedicated for non-VSP connections.

Note: An upper-case *CONNECT* implies a VSP connection.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

discon hIdx,reason

This indicates that the connection identified by the handle *hIdx* was dropped and the reason for disconnection is specified by the integer value *reason*. See source code for the *smart*BASIC application for *reason* values by searching for the string CONN_ERROR_

encrypt hIdx

Indicates that the connection identified by the handle *hIdx* has entered the encrypted state.

FC:hIdx, hAttr, props

Triggered by the AT+GCFA command to search for a characteristic's attribute handle.

- *hIdx* – Connection handle index
- *hAttr* – The handle of the attribute, if found. Otherwise, it is *0*.
- *props* – The property bitmask of that characteristic

Note: hAttr==0 if characteristic not found.

FD:hIdx, hAttr

Triggered by the AT+GCFA command to search for a descriptor's attribute handle.

- *hIdx* – Connection handle index
- *hAttr* – The handle of the attribute, if found. Otherwise, it is *0*.

Note: hAttr==0 if characteristic not found.

IN:hIdx, hAttr, hexdatastring

This message happens asynchronously when a remote GATT server sends this device a notification or an indication where:

- *hIdx* – Server connection
- *hAttr* – The handle of the attribute that was updated with the new data in *hexdatastring* which is in hexadecimal format.

Note: If it is an indication then a GATT acknowledgement has been automatically sent.

MT:h size

These messages may occur asynchronously after the AT+LMTU command is entered while in non-VSP mode.

- *h* – Connection handle index
- *size* – The maximum size of data that can be sent using the +GCWA and +GCWC commands

NOCARRIER 0

While pairing, if the I/O capability Sreg107 is appropriate and the other end also has a user interface, this could be sent to the host to request a 32 hex characters string which it then submits using the AT+PRSP command

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

PU:h phytx phyrx
PF:h status

These messages occur asynchronously after the AT+LMTU command is entered while in non-vsp mode. PS is when the PHY negotiation was successful and PF when it failed.

- *h* – Connection handle index
- *phytx* – The PHY for transmit, 1 for 1MPHY, 2 for 2MPHY and 4 for CodedPHY
- *phyrx* – The PHY for receive, 1 for 1MPHY, 2 for 2MPHY and 4 for CodedPHY
- *status* – The status code when negotiation failed.

passkey?

While pairing, if the I/O capability Sreg107 is appropriate and the other end also has a user interface, this could be sent to the host to request an integer value in the range 0 to 999999 which it then submits using the AT+PRSP command.

RING address,[U|T]

When waiting for a VSP connection, this message is the first indication to the host that a connection is in progress from a device with MAC address.

The [U|T] implies either a *U* which implies that the *address* is not in the trusted device database or a *T* which implies the incoming VSP connection is from a trusted device

SC:i, newValue

This message occurs asynchronously when a remote GATT client writes into a SCCD descriptor of one of the local characteristics identified by *I* (which is provided as a result of AT+GSCE when the characteristic was created and committed). The parameter *newValue* is an integer.

See responses *WR* and *CC* when the characteristic value and CCCD are written.

showcode passcode

While pairing, if the I/O capability Sreg107 is appropriate and the other end also has a user interface, this could be sent to the host to display the integer value *passcode* as a six-digit decimal number with trailing 0's so that a six-digit number is shown. This end must confirm with a Yes or No to complete the pairing and that is done using the command AT+PRSP

Scanned

When waiting for an incoming VSP connection, it is possible to also scan for adverts for a specified interval using the command AT+LSCN. This then triggers advert report *AD*. When the scan times-out, this response is sent to the host.

WR:i, hexdatastring

This message occurs asynchronously when a remote GATT client writes into one of the local characteristics identified by *i* which was provided as a result of AT+GSCE when the characteristic was created and committed. The parameter *hexdatastring* is the new data that was written into the characteristic.

See responses *SC* and *CC* when the SCCD and CCCD are written.

xxkey?

While pairing, if the I/O capability Sreg107 is appropriate and you receive this, contact Laird. This is to cater for a future pairing authentication scheme. The API allows for this as a hypothetical future scenario

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.6 AT Commands (NFC Operation)

This section describes the commands for NFC operation.

When an active NFC coil energises or de-ernergises this module's NFC coil, an asynchronous response is sent to the host. And, if the tag is successfully read or written by the active NFC device, an appropriate asynchronous response is also sent. See a full description of these responses in the section *Responses (NFC Operation)* in the next sub-chapter.

In this section the word 'record' has a specific meaning as defined in the NFC specification.

AT+NOPN (Open NFC interface)

Command	`AT+NOPN max_ndef_buflen <,writeable>`
Description	Open the NFC interface and reserve `max_ndef_buflen` bytes of memory to create an NDEF message which can contain multiple records as long as there is memory to accommodate them. If the optional <,writeable> is not present then the tag is read only. If it is present and has a value of 1, then it will writable when the underlying firmware in the module allows that. When write capability is absent it will only open in readonly mode. The argument `max_ndef_buflen` should be within the range 128 to 512 and it can be changed by modifying the values of the #defines `NFC_MIN_TAG_SIZE` and `NFC_MAX_TAG_SIZE` appropriately in the .sb file.
Possible Responses	`"OK"` `"ERROR"`

AT+NCLS (Close NFC interface)

Command	`AT+NCLS`
Description	Close the NFC interface and all memory previosly reserved is released
Possible Responses	`"OK"` `"ERROR"`

AT+NRST (Clear NDEF message buffer)

Command	`AT+NRST`
Description	Reset the NDEF message buffer so that is marked as empty, so that a new message can be added using the commands AT+NRAT and AT+NRAG
Possible Responses	`"OK"` `"ERROR"`

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+NRAT (Add Text Type Record to NDEF buffer)

Command	`AT+NRAT "lang","message"`
Description	Add a Text type record to the NDEF message buffer that was made available via AT+NOPN. For this record the NTF type will be se to 0x01 and the 'type' field in the record header will be set to the string value "T". The ID field in the header will be set as empty. The "lang" argument is a laguage specifier formatted so that the first character is the length of the string specifying the language. So for example, to specify that the message is in English use "\02en" where the three character \02 sequence will be escaped into 2 and 'en' the abbreviation for English. The "message" argument is any message and you can add UTF-8 strings by adding appropriate escape sequence for non-printable bytes.
Possible Responses	`"OK"` `"ERROR"`

AT+NRAG (Add Generic Type Record to NDEF buffer)

Command	`AT+NRAG tnf,"type","id","payload"`
Description	This command is used to add any record to the message as all the fields in the header and the payload can be explicitly specified. The record type is specified via the 'tnf' argument. The tnf value in the first byte of the ndef record header shall be in the range 0 to 7 as per the NDEF specification. The "type" value is written to the type field in the header. The "id" value will populate the ID field in the header and can be specified as empty using an empty double quoted string "". The payload of the ndef record is populated byt "payload". Note that any of the 3 string arguments can have non-prontable characters by escaping such values with the three character sequence \hh where hh are the 2 hex digits required to fully spcify an eight bit value.
Possible Responses	`"OK"` `"ERROR"`

AT+NCMT (Commit NDEF message buffer)

Command	`AT+NCMT`
Description	Commit NDEF message buffer to the NFC stack so that it can be made available to a reader
Possible Responses	`"OK"` `"ERROR"`

AT+NSEN (Enable NFC coil sensing)

Command	`AT+NSEN`
Description	Enable the NFC coil so that an active reader/writer can access the ndef message that was commited using the most recent AT+NCMT command
Possible Responses	`"OK"` `"ERROR"`

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

AT+NSDS (Disable NFC coil sensing)

Command	AT+NSDS
Description	Disable the NFC coil so that an active reader/writer cannot access the ndef message so that a new message can be committed if required.
Possible Responses	"OK" "ERROR"

3.7 Responses (NFC Operation)

This section describes all the responses generated by the module related to NFC operation and only if that feature is compile time enabled when the *smart*BASIC application is loaded into the module.

To simplify reception of messages in the receiving device, each message starts with a \n character and ends with a \r character.

After stripping the \n start character, each response starts with a *unique* two-character sequence to help the host decode the response in a stateless manner.

Some responses are synchronous which mean they are used to terminate a command so that the command parser can process more commands and some that are asynchrnous, meaning they can happen at any time.

However please note that if there is an ongoing VSP connection and so data is being transparently bridged between the UART and air-interface, then all NFC related asynchrononous messages are suppressed and the only way to know after the VSP connection ceases is via the counts returned by ATI50 and ATI51

3.7.1 Response: Synchronous and Terminating

When a host receives these responses it can issue new commands and expect them to be processed immediately.

ERROR nn

A command was not successfully actioned and *nn* is an error code. The error codes are as follows:

- 60 – NFC not open
- 61 – NFC NDEF message empty
- XX : Other Generic Errors (See earlier section)

OK

A command was successfully expedited.

3.7.2 Response: Synchronous and Not Terminating

When a host receives these responses, it cannot issue new commands and expects them to be processed immediately as a terminating response is still to come.

None have yet been defined.

3.7.3 Response: Asynchronous

A host must be designed to expect any of these responses at any time. To help with enabling a host to be as stateless as possible, all these responses have a unique 2 letter starting sequence to quickly determine what it means and how it gets processed.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

NS:state

This message is asynchronously sent when an active NFC device energises or de-energises this modules NFC coil. *State* is as follows:

- 1 – Energize
- 2 – De-energize

NR

These message occur asynchronously when the tag committed using AT+NCMT is successfully read by an active NFC reader

3.8 Compile Time Default Behavior

This AT interface behavior is supplied in source format. You are free and encouraged to modify and enhance as desired.

Behavior may be altered by altering the values of #defines at the top of the source code file called *$autorun$.AT.interface.xxx.yyy.zzz.sb* which includes the file *LIB.AT.interface.sb*.

Where xxx.yyy.zzz is some descriptive text to help you maintain several versions of the application in your source repository.

Noteworthy definitions are as follows:

ATI_RESPONSE_0

This is a small string which is returned for command ATI0

ATI_RESPONSE_10

This is a small string which is returned for command ATI10

MAX_CONNECTIONS

This is currently set to *8* but you can reduce it to ease the pressure on memory usage.

MAX_CHARACTERISTICS

This is currently set to *24*. This defines the maximum number of characteristics that can be added using the AT+GSCE command.

CONN_INTERVAL_MIN_ASPERIPH_US

CONN_INTERVAL_MAX_ASPERIPH_US

These are minimum and maximum connection intervals as a peripheral. The module accepts anything that is provided and it does not trigger a connection parameter renegotiation.

NFC_MIN_TAG_SIZE

NFC_MAX_TAG_SIZE

These are the minimum and maximum buffer sizes with which the NFC interface can be opened in which to save one or more NDEF messages.

MaxDevNameSize

The maximum allowable size of the advertised device name. It should not be set to larger than 20.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

MaxCmdStringSize

The maximum allowable size of a single AT command line in terms of characters. This includes the terminating \r character.

3.9 Low Power UART Operation

This application, by its very nature, requires a host to control it by sending AT commands over the UART interface given it operates like a modem.

The UART interface that is embedded inside the nrf52840 microcontroller at the heart of the Laird module consumes about 300 to 400 microamps when it is open.

We have demonstrated that it is possible to operate the nrf52840 microcontroller in **doze** mode so that the total current consumption can be sub 30 microamps (when HL7800 is in deep sleep mode).

Note: Overall, the total current consumed is the sum of the current drawn by the nrf52840 and the HL7800 modem.

Using BLE (a low-power radio technology), the radio chip is optimized so that, in between radio events, it can go to sleep. Because of this, a typical power profile can show a doze current of sub 10 uA and about 8000 microamps when there is a radio event (which can be a few 10s of microseconds in length to over 1000 microseconds. Also, the radio event can occur as quickly as 7500 microseconds and as slow as over 4000000 microseconds.

Similarly, the HL7800 can be in PSM or eDRX mode; it consumes very low currents when hibernating, but current as high as 130 ***milli***Amps when the cellular radio is active.

This shows that the duty cycle of low to high power provides for overall low average current consumption and when the HL7800 is in hibernate mode, the nrf52840's consumption of 300 to 400 microamps is significant.

This requires a ***cooperative*** existence with the host which means an extra GPIO line is connected between the host and the module which is used to manage the open/close operation of the module's UART.

This GPIO, which is a digital output from the UART host (referred to as *Keep UART Open* line in this section) is, by default, connected to the nrf52840's GPIO input line P0.02 which is on pin M2.59 on the edge connector.

The AT Interface app is crafted so that, if it sees the *Keep UART Open* high, it does ***not*** try to close both UARTs automatically. Otherwise, when low, if there was no UART activity for a default time of five seconds, it automatically closes both UARTs to reduce the current consumption. While the UARTs are closed, if there is incoming data from over BLE that must be relayed to the host, it sautomatically open the UARTs, sends the data, and starts a shutdown timer. The default timeout of five seconds can be changed via the SRegister 213. After a change, it requires a save using AT&W because the SRegister ***is only read on power up*** or a reset invoked by the command ATZ.

When the UARTs are automatically shut down, it de-asserts the RTS line. This is a signal to the serial port of the host that it should stop sending data. It also makes the RTS line of the AUX port connected to the HL78 an input so that the pull-up resistor on that pin in the HL7800 de-asserts it. If the host sees that the module's RTS is de-asserted (which it detects via its own CTS input line) and that it has set the *Keep UART Open* line low, it can set that line high. This results in the RTS line being reasserted after the module re-opens the UART and so that data can be received by the module.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.10 Application State Machines

3.10.1 Idle and Scanning

Notes:
(1) States in **BLUE** respond to AT commands, otherwise parser is suspended

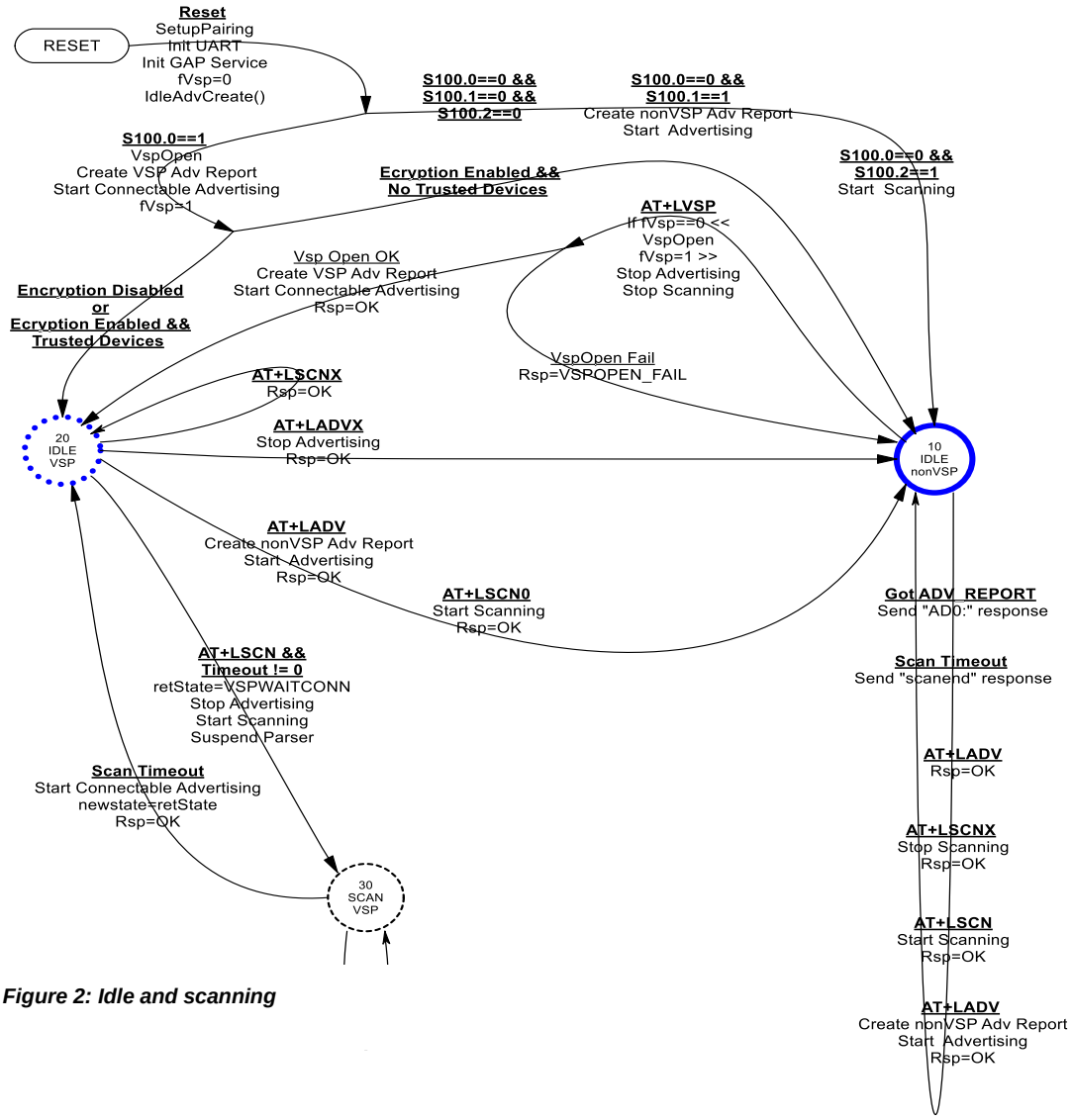


Figure 2: Idle and scanning

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.10.2 Outgoing VSP Connection

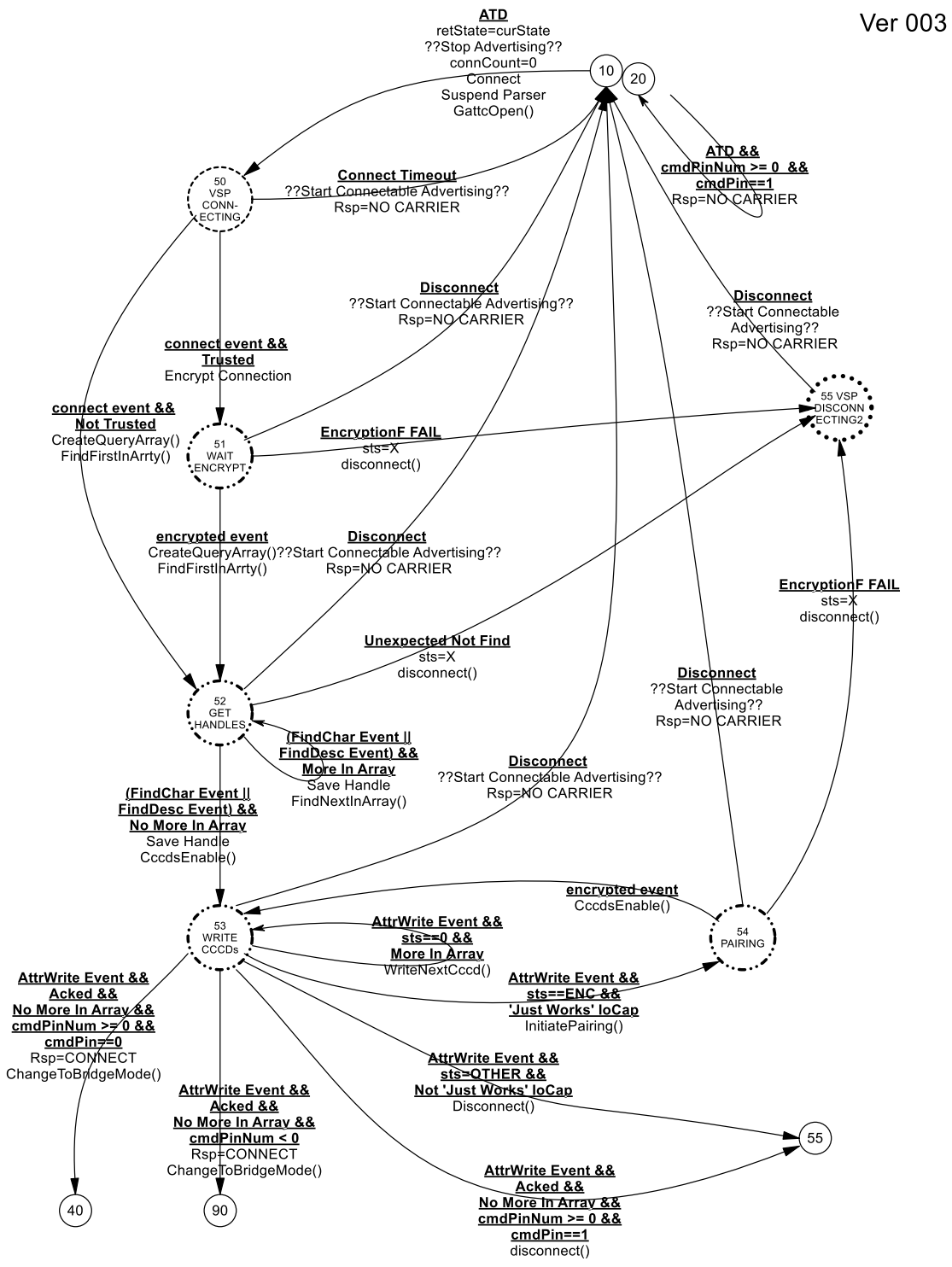


Figure 3: Outgoing VSP Connection (not in BL600)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.10.3 Incoming VSP Connection

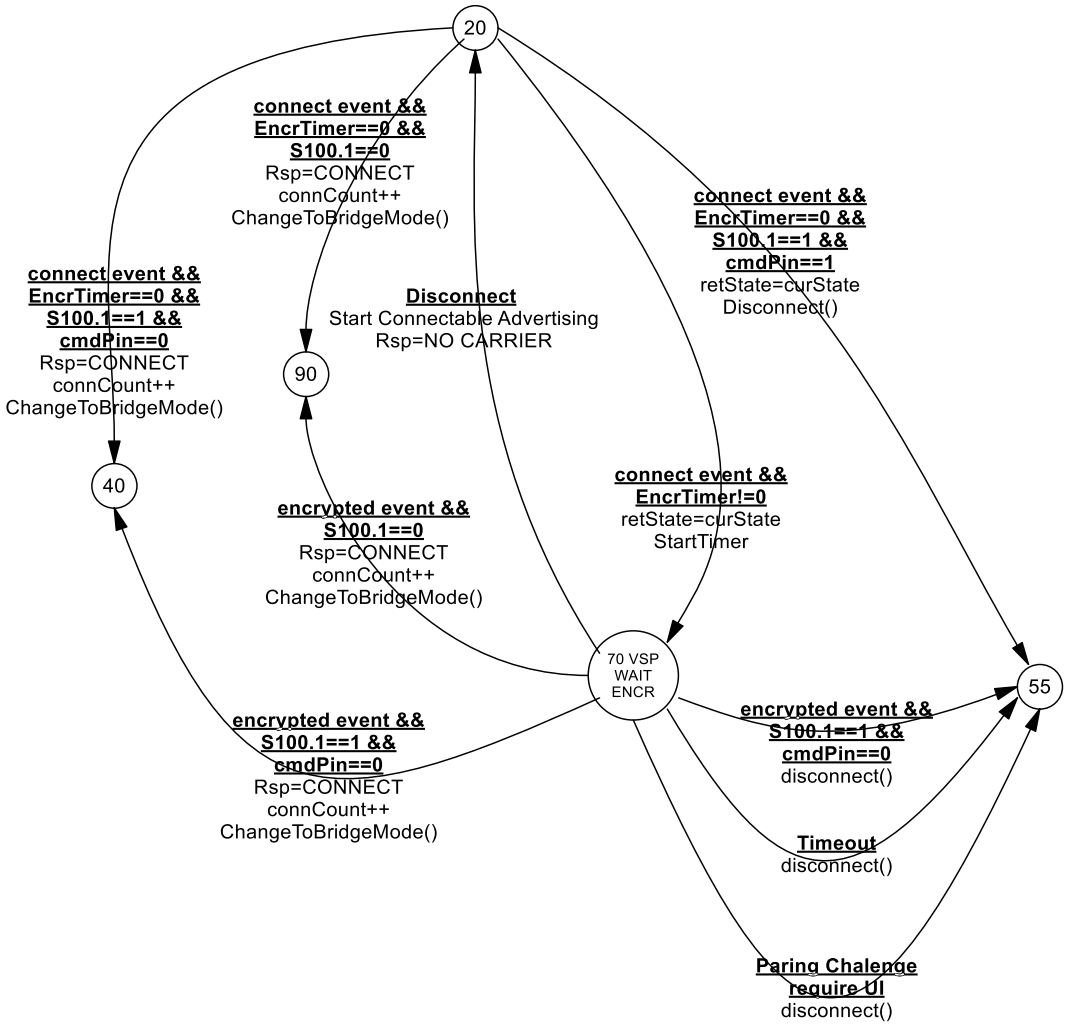


Figure 4: Incoming VSP Connection

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.10.4 Outgoing and Incoming non-VSP Connection

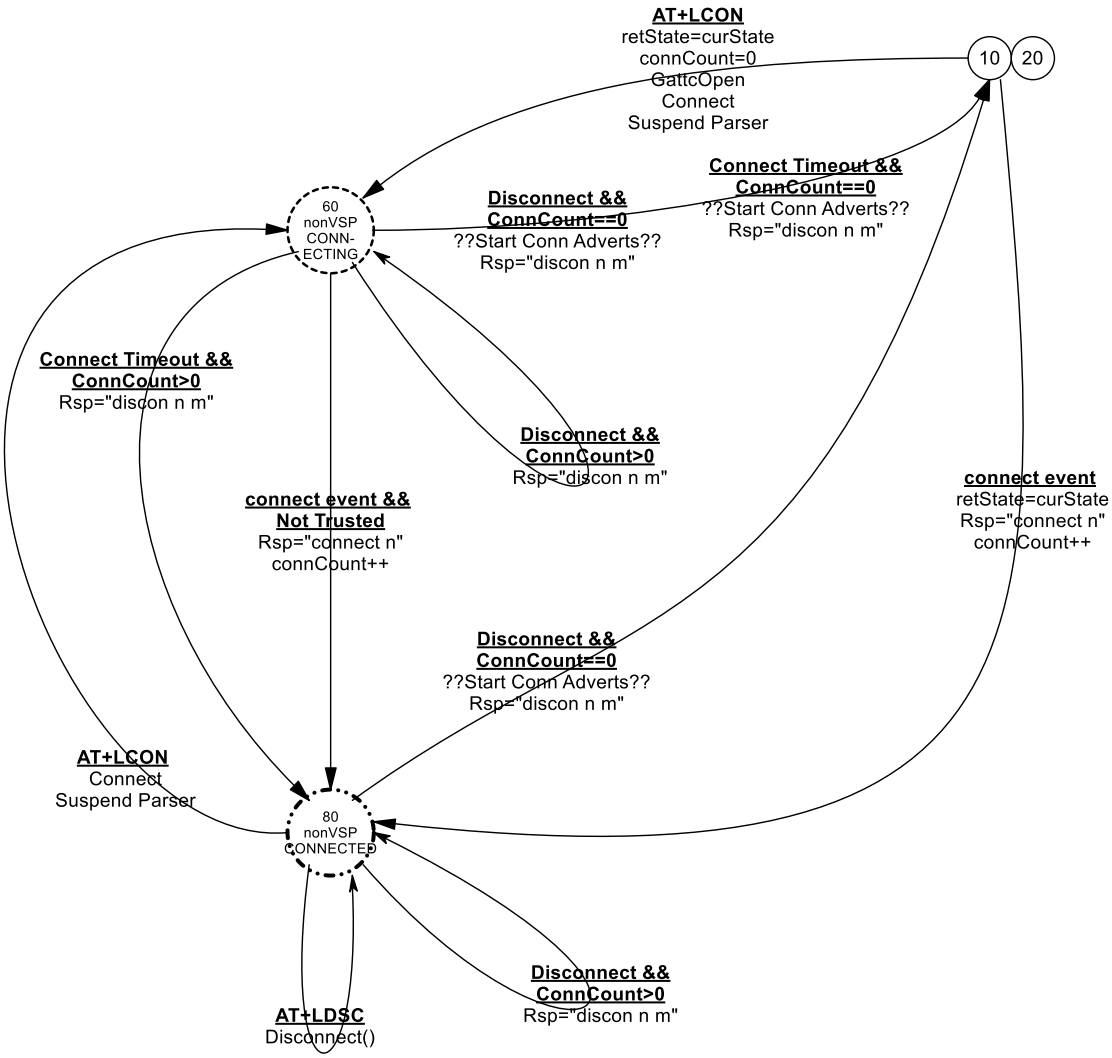
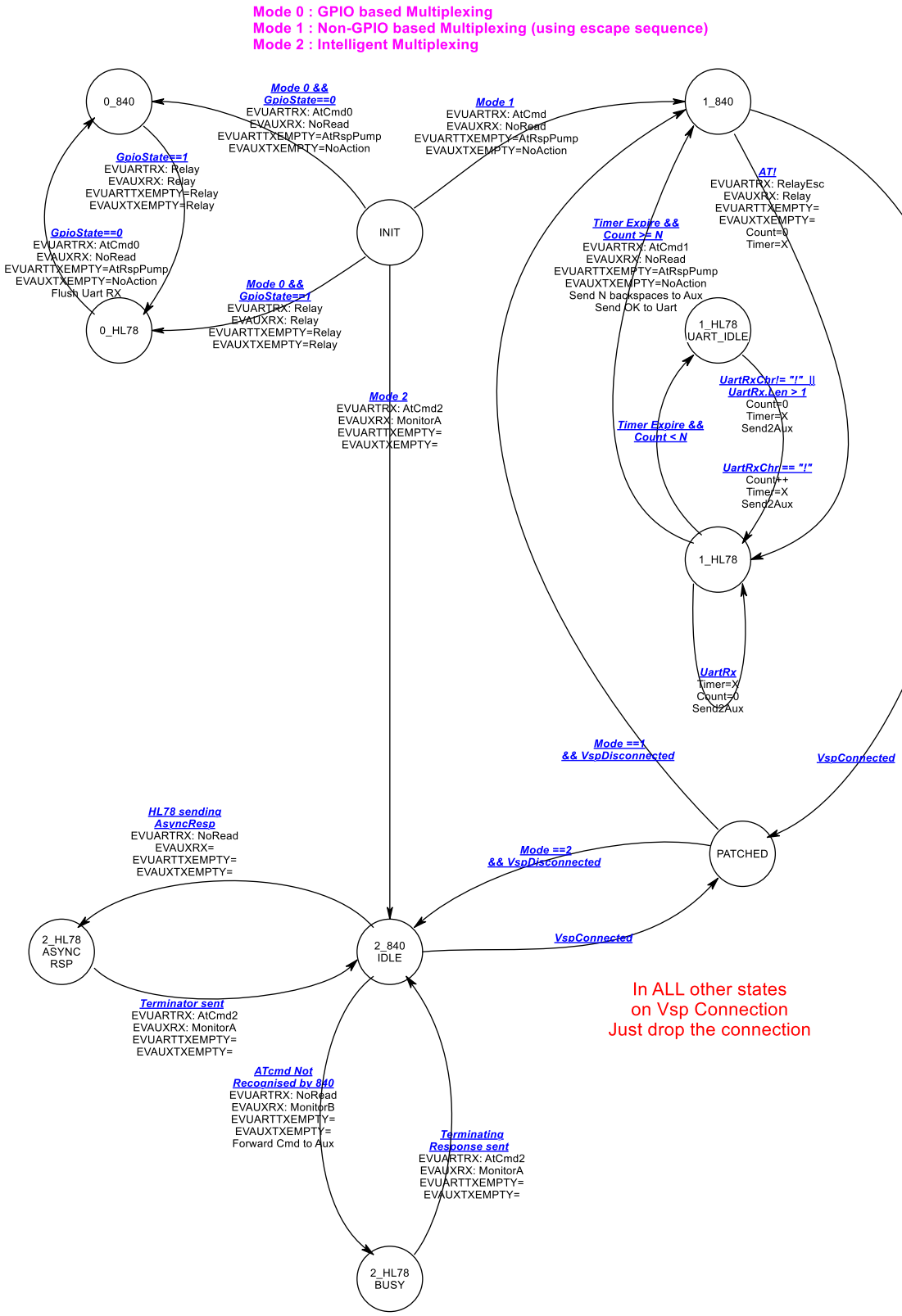


Figure 5: Outgoing and Incoming Non-VSP Connection

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.10.5 Uart Multiplexer Mode State Machine



Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610