Alps Virtual Cable Light Firmware Revision B3_10 Release Note

Document Version 1.0

Important Notes

The information contained in this document is confidential, which shall not be provided to any third parties without prior agreement notice.

Contents

1 Limitation of Liability 2
2 Introduction 2
3 Qualification Status 2
4 Firmware Change History 3
4.1 Changes Relative to Alpha1 3
4.2 Changes Relative to Alpha2 3
4.3 Changes Relative to Alpha3 3
4.4 Changes Relative to Alpha4 3
4.5 Changes Relative to Alpha5 3
4.6 Changes Relative to Alpha6 3
4.7 Changes Relative to Alpha7 3
4.8 Changes Relative to Alpha7.1 3
4.9 Changes Relative to Alpha8 3
4.10 Changes Relative to Beta1 4
4.11 Changes Relative to Beta2 4
5 Functionality 4
5.1 State Diagram 5
5.2 Serial Port Profile 5
5.3 Dial-up Networking Profile Hosting 6
5.4 Headset Profile 6
5.5 Hands-Free Profile 6
5.6 Object Push Profile Hosting 7
6 System Configuration 7
6.1 Connections 7
6.2 Inquiry Scan Activity 7
6.3 Page Scan Activity 7
6.4 Security 8
6.5 Sniff Mode 8
6.6 Park Mode 8
6.7 Hold Mode 8
6.8 Device Local Name 8
6.9 Class Of Device 8
6.10 Timers 8
6.11 RFCOMM 8
6.12 Bluetooth Supported Features 9
7 Host Interface 9
7.1 UART Data Discrimination 9
7.2 UART Physical Specification 9
7.3 UART Logical Specification 10
7.4 UART Configuration 10
8 Security Policy 11
9 Test Features 11
9.1 Bluetooth Test Mode 11
9.2 Link Condition 12
9.2.1 Received Signal Strength Indication 12
9.2.2 Link Quality 12
10 Persistent Store 12
10.1 Automatic Defrag 13
10.2 Forced Defrag 13
11 Programmable Input / Output 13
12 Known Issues / Outstanding Items 14
13 References 14
14 Document Change History 14
14.1 Alpha Version 14

14.2 Beta Version 14
14.3 Official Version 14
15 Test Results 15
15.1 AT Command tests 15
15.2 AT Command parameter boundary tests 17
15.3 Bulk File Transfer 19
15.3.1 Test Conditions 19
15.3.2 Test Results 19
15.4 Functional tests 20
15.4.1 Establish and Release Service Connection 20
15.4.2 Inquiry 20
15.4.3 Establish and Release SCO Connection 20
15.4.4 Register/Unregister a Remote Device to/from the Security Database 20
15.4.5 Pair with Remote Device 20
15.4.6 Low Power Modes 21
15.5 Throughput Measurement 22
15.5.1 Test Conditions 22
15.5.2 Test Results 22
15.6 Latency measurement 24
15.6.1 Test Conditions 24
15.6.2 Test Results 24
15.7 Power consumption (UGXZ2) 25
15.7.1 Idle State 25
15.7.2 Inquiring and Paging State 25
15.7.3 Discoverable and Connectable State 25
15.7.4 RFCOMM Connected State 25
15.8 Power consumption (UGPZ 1) 26
15.8.1 Idle State 26
15.8.2 Inquiring and Paging State 26
15.8.3 Discoverable and Connectable State 26
15.8.4 RFCOMM Connected State 26
15.9 Interoperability Testing 27
15.9.1 Interoperability Test Procedure 27
15.9.2 Test Results 27

1 Limitation of Liability

The firmware described in this document is suitable for use only with Alps Bluetooth module. It is the responsibility of the user to determine if the firmware is appropriate for production. Primary target usage is evaluation and demonstration.

Alps makes no warranty or representation whatsoever of merchantability or fitness of this firmware for any particular purpose or use. In no event shall Alps be liable for any consequential, incidental or special damages whatsoever arising out of the use of, or inability to use this firmware even if the user has advised Alps of the possibility of such damages. The user assumes any and all risks associated with the use of the firmware and shall indemnify, defend and hold Alps harmless from third party claims arising from use of the firmware.

2 Introduction

This document presents a description of the Alps Virtual Cable Light firmware Revision B3_10 implementing all Bluetooth core protocols up to RFCOMM and profiles associated with a fully functional Audio Gateway implementation. The supported profiles are discussed in the Functionality section.

The firmware is solely compatible with specific Alps Bluetooth modules. Descriptions in this document focus on the Bluetooth implementation and non-Bluetooth related features as opposed to the Bluetooth specification itself. For this reason it is assumed that the reader is familiar with the major functionality of Bluetooth devices.

3 Qualification Status

The Alps Virtual Cable Light is layered above pre-qualified components that do not have to be re-qualified when the VCL is qualified. Alps can provide assistance in gaining qualification for profiles including relevant tests, paperwork and recommended BQB.

4 Firmware Change History

4.1 Changes Relative to Alpha1

- Change local name command *AT+BNAM* so that it accepts any ASCII characters.
- Addition of *+BCUS* result code that contains custom AT Commands sent from the peer Headset or Handsfree device.
- Addition of *AT+BCUS* command to enable host to send custom AT Commands to the peer Headset or Handsfree device.
- All result codes now take the form *<CR><LF>+BXXX<CR><LF>* where *<CR>* is the Carriage Return character and *<LF>* is the Line Feed character.
- AT Commands received from host are parsed as soon as the terminating *<CR>* character is received. Previously, at least 4 characters were needed to kick off the parser.
- PIN code requests while in a state other than pairing (using *AT+BPRS* or *AT+BPRM*) are automatically rejected.
- Addition of feature to allow rejection of PIN code requests using the *AT+BPIN* command.
- Addition of feature to supply link keys to the module for authentication.
- Security database commands added; add and remove peer device.
- *AT+BACN* command for SCO connection attempts now includes packet type setting.
- Removed all references to connection handles from result codes and commands.

4.2 Changes Relative to Alpha2

- Addition of *AT+BEVT* commands to enable/disable event reporting by the firmware. Refer to the AT Command Reference document for more details.
- Result codes *+BSPK* and *+BMIC* changed to *+BVGS* and *+BVGM* respectively to match the corresponding AT Commands.
- *+BVGS* and *+BVGM* result code parameters are now expressed in hexadecimal instead of decimal.
- AT command parser error handling fixed so unexpected reboots due to illegal commands are eliminated.
- Buffering of OPP packets received over the UART implemented in the module to improve interoperability with non-compliant stacks.
- UART echo mechanism fixed so that every command character is echoed.
- OPP service record changed to indicate that all object formats are supported.

4.3 Changes Relative to Alpha3

- Upgraded development platform.
- Fixed connect as master bug where if the SDP search failed, the ACL connection would not be released.
- Fixed *AT+CLIP* parse bug for Hands-Free service.
- Fixed UART Ÿ RFCOMM data transfer deadlock bug found at UART baudrates above 115200bps.

4.4 Changes Relative to Alpha4

- Added feature to enable UART configuration from the host using AT Commands.

4.5 Changes Relative to Alpha5

- Changes made to error reporting.
- Event masking command *AT+BEVT* extended to support masking of warnings.

4.6 Changes Relative to Alpha6

- Added dynamic registration of service records.
- Added commands to configure inquiry/page scan parameters and sniff mode parameters.

4.7 Changes Relative to Alpha7

- Fixed result code *+BRFC* after connecting to the peer device.
- Fixed send result code *+BRFC* after the data to the UART when connect to the peer device.
- Fixed be not able to send or receive the data on UGXZ4-Flash.

4.8 Changes Relative to Alpha7.1

- Changed inquiry filter using the Class Of Device.
- Added function to configure the initial Modem Status Command.
- Added command to configure the module's security mode.
- Supported to enter the hold mode and to write link policy.
- Disabled UART echo by default.
- Added command to enable device under test mode.

4.9 Changes Relative to Alpha8

- Disabled Master/Slave switch.
- Fixed send a parse ok/error result code after a system error result code when send a command.

4.10 Changes Relative to Beta1

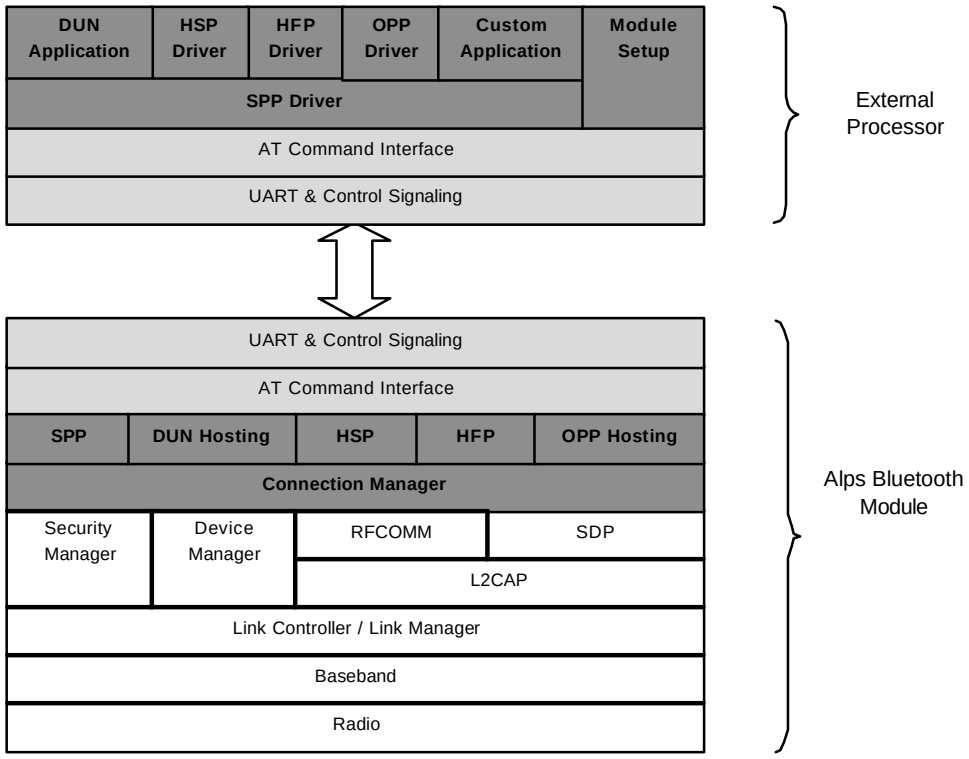
- Not Supported the Fax Profile.
- Fixed *AT+BINQ* bug that the module reboots by issuing this command continuously.
- Fixed *+BRFC* result code parameter for the OPP service.
- Added command to indicate the "call_setup" for the HFP.
- Fixed *AT+BINP* bug that the module reboots by issuing this command continuously when this command is unexpected.
- Changed *AT+BSEC* features that authentication and encryption are always enabled for the DUN service at least.

4.11 Changes Relative to Beta2

- Supported Hands-Free Profile Adopted Version1.0.
- Added command to write the local Class Of Device.
- Added command to change the UART recovery timer.
- Added command to tune the UART for throughput or latency.
- Added command to force defragmentation of the flash ROM.
- Added read commands to obtain the current settings.
- Sniff mode can now be used when a SCO connection exists.
- Enabled Master/Slave switch.

5 Functionality

The following diagram shows the functionality of the firmware and how it should be integrated with an external host. The firmware supports all of the Bluetooth version 1.1 core protocol layers up to and including RFCOMM in addition to the following Bluetooth profiles; Serial Port Profile (SPP), Dialup Networking Profile (DUN), Headset Profile (HSP), Hands-Free Profile (HFP) and Object Push Profile (OPP). Note that in several cases the profile is actually 'hosted' by the firmware with the profile functionality residing on an external host processor.



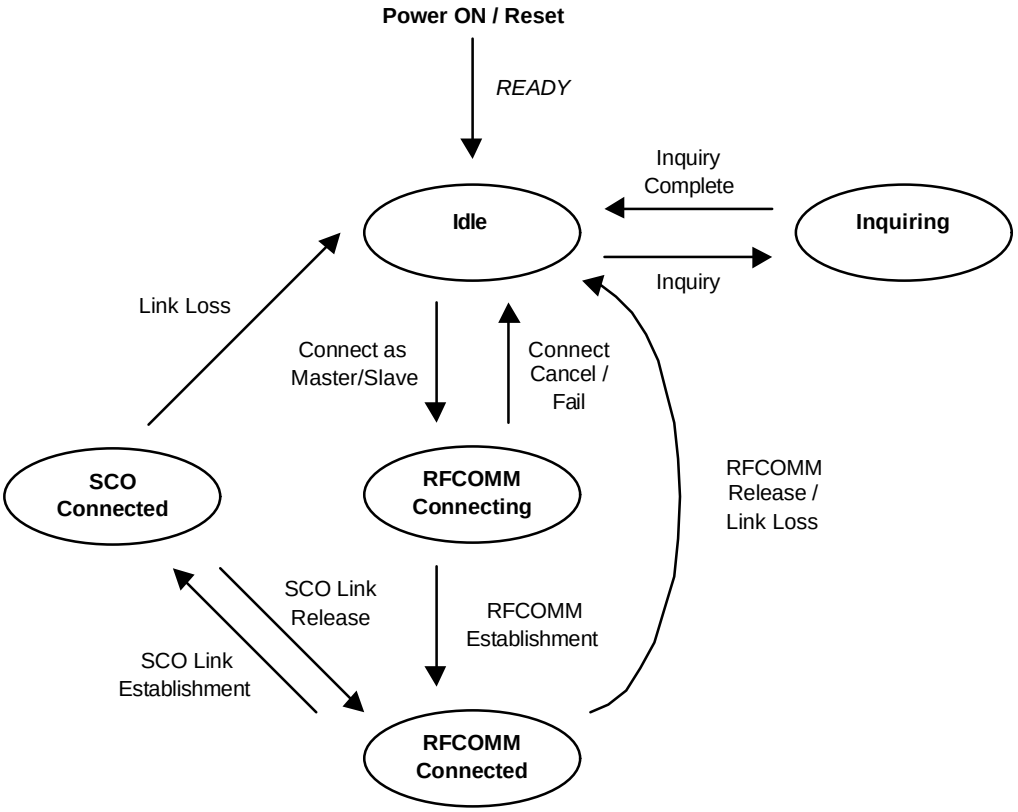
With the exception of the Security Manager and Device Manager, the white blocks in the diagram depict the Bluetooth core entities. The Security Manager allows the module to control the security of the device based upon the Bluetooth Security White Paper and also provides a security database that can be used to manage the security related information of all remote Bluetooth devices encountered. The Device Manager provides an interface similar to the Bluetooth defined Host Controller Interface (HCI) that may be used to communicate with the lower Bluetooth protocol layers. Access to the Bluetooth protocol layers and the Security/Device Managers is made possible through the Connection Manager layer.

The diagram indicates that the DUN and OPP profiles are actually hosted by the firmware. The profile functionality needs to be implemented on an external processor in the form of an application. Other profile functionality is implemented by the firmware and simply requires a driver on the external processor to function correctly. Note that custom applications can be implemented on top of the SPP profile that do not have to conform to any of the Bluetooth specifications.

The interface between the Bluetooth module and the external host processor is UART based. Several additional signals are required to discriminate between data and commands but the operation is relatively simple. Communication between the firmware and the application running on the external processor takes the form of AT Commands, information responses and Result Codes similar to that used by a PC to communicate with a dialup modem.

5.1 State Diagram

The diagram below shows the firmware state transitions and the events that trigger those transitions.



5.2 Serial Port Profile

The SPP functionality has been written against the Bluetooth Profiles Specification, volume 2, v 1.1, February 22nd 2001, Part K:5 that specifies requirements for devices claiming compliance with the Serial Port Profile. The firmware complies with the specification for devices performing the role of Dev A and Dev B. The service record is defined as follows:

Parameter	Default	Configurable	Comments
Type	SerialPort	No	
Attributes defined	ServiceClassIDList ProtocolDescriptorList LanguageBaseIDList ServiceName	No	
Service name	"Serial Port"	No	
RFCOMM server channel	Variable	No	
UUID type	16bit	No	
L2CAP Maximum Transmission Unit (MTU) for SDP connections	48bytes	No	In certain cases the SDP packets will exceed the L2CAP MTU so the remote device must support the SDP continuation flag.
Service record language base	English	No	

5.3 Dial-up Networking Profile Hosting

Due to resource limitations it is currently not possible to implement an embedded Dialup application on the module. The service record, however, is hosted by the firmware so it is possible for peer devices to discover the DUN service as normal. The actual DUN functionality must reside on the external processor with all DUN related data transferred over the UART. This is basically the same as the SPP operation in that the DUN data will be simply treated as user data. The DUN functionality should only comply with the Bluetooth specification for devices performing the role of Gateway (GW). The service record is partially configurable and is currently defined as follows:

Parameter	Default	Configurable	Comments
Type	DialupNetworking	No	
Attributes defined	ServiceClassIDList ProtocolDescriptorList BluetoothProfileDescriptorList AudioFeedbackSupport ServiceName	No	
Service name	"Dialup"	No	
RFCOMM server channel	Variable	No	
UUID type	16bit	No	
L2CAP Maximum Transmission Unit (MTU) for SDP connections	48bytes	No	In certain cases the SDP packets will exceed the L2CAP MTU so the remote device must support the SDP continuation flag.
Audio Feedback Support	-	Yes	AT+BRSR used to set this parameter.

5.4 Headset Profile

The HSP functionality has been written against the Bluetooth Profiles Specification, volume 2, v 1.1, February 22nd 2001, Part K:6 that specifies requirements for devices claiming compliance with the Headset Profile. The firmware complies with the specification for devices performing the role of Audio Gateway (AG) only. The service record is defined as follows:

Parameter	Default	Configurable	Comments
Type	HeadsetAudioGateway	No	
Attributes defined	ServiceClassIDList ProtocolDescriptorList BluetoothProfileDescriptorList ServiceName	No	
Service name	"Voice Gateway"	No	
RFCOMM server channel	Variable	No	
UUID type	16bit	No	
L2CAP Maximum Transmission Unit (MTU) for SDP connections	48bytes	No	In certain cases the SDP packets will exceed the L2CAP MTU so the remote device must support the SDP continuation flag.

5.5 Hands-Free Profile

The HFP functionality has been written against the Bluetooth Hands-Free Profile, adopted version 1.0, April 29th 2003 that specifies requirements for devices claiming compliance with the Hands-Free Profile. The firmware complies with the specification for devices performing the role of Audio Gateway (AG) only. The service record is partially configurable and is currently defined as follows:

Parameter	Default	Configurable	Comments
Type	HandsfreeAudioGateway	No	
Attributes defined	ServiceClassIDList ProtocolDescriptorList BluetoothProfileDescriptorList ServiceName Network SupportedFeatures	No	
Service name	"Voice Gateway"	No	
RFCOMM server channel	Variable	No	
UUID type	16bit	No	
L2CAP Maximum Transmission Unit (MTU) for SDP connections	48bytes	No	In certain cases the SDP packets will exceed the L2CAP MTU so the remote device must support the SDP continuation flag.
Network type	-	Yes	AT+BRSR used to set this parameter.
Supported Features	-	Yes	AT+BRSR used to set this parameter.

5.6 Object Push Profile Hosting

Due to resource limitations it is currently not possible to implement an embedded Object Push Profile (OPP) on the module. The service record, however, is hosted by the firmware so it is possible for peer devices to discover the OPP service as normal. The OPP functionality must reside on the external processor with all OBEX data transferred over the UART. This is basically the same as the SPP operation in that the OBEX data will be simply treated as user data. The service record is partially configurable and is currently defined as follows:

Parameter	Default	Configurable	Comments
Type	OBEXObjectPush	No	
Attributes defined	ServiceClassIDList ProtocolDescriptorList ServiceName Network SupportedFeatures	No	
Service name	"Object Push"	No	
RFCOMM server channel	Variable	No	
UUID type	16bit	No	
L2CAP Maximum Transmission Unit (MTU) for SDP connections	48bytes	No	In certain cases the SDP packets will exceed the L2CAP MTU so the remote device must support the SDP continuation flag.
Supported Formats	-	Yes	AT+BRSR used to set this parameter.

When the OPP service is connected, all data received over the UART will be buffered into complete OBEX packets before being transmitted over RFCOMM to the peer device. The reason for this is that several commercial Bluetooth stacks cannot parse OBEX packets spanning several RFCOMM frames. It is believed that this non-compliance of the relevant Bluetooth profile.

6 System Configuration

Many of the system parameters are configurable in order to meet the needs of individual applications. Parameters that reside in non-volatile memory must be configured every time the module reboots whereas others that reside in flash ROM only have to be configured once.

6.1 Connections

Parameter	Default	Configurable	Comments
Timeout	None	No	Page Timeout is 5s. But connection attempt is continued until this operation is cancelled.
Allowed remote device	Any	No	Connection attempts from all remote devices will be accepted as long as the security requirements are fulfilled.
Link Supervision Timeout	5s	No	Bluetooth connection slaves cannot change the Link Supervision Timeout value. It is the responsibility of the connection master to make changes as required.

6.2 Inquiry Scan Activity

Parameter	Default	Configurable	Comments
Window	0x0012 (11.25ms)	Yes	AT+BSSP used to configure this parameter.
Interval	0x0800 (1280ms)	Yes	AT+BSSP used to configure this parameter.
Inquiry Access Code	General (0x9E8B33)	No	Inquiring masters must use this access code in order to discover the local device.

Inquiry scan is disabled as long as an active Bluetooth connection exists.

6.3 Page Scan Activity

Parameter	Default	Configurable	Comments
Window	0x0050 (50ms)	Yes	AT+BSSP used to configure this parameter.
Interval	0x0400 (640ms)	Yes	AT+BSSP used to configure this parameter.

Page scan is disabled as long as an active Bluetooth connection exists.

6.4 Security

Parameter	Default	Configurable	Comments
Security mode	Non-secure	Yes	AT+BSEC used to configure this parameter.
Authentication	Off	Yes	AT+BSEC used to configure this parameter.
Authorization	Off	No	
Encryption	Off	Yes	AT+BSEC used to configure this parameter.
Minimum encryption key length	8bit	No	
Maximum encryption key length	56bit	No	

Further security details can be found in the Security Policy section of this document.

6.5 Sniff Mode

Parameter	Default	Configurable	Comments
Maximum interval	0x0100	Yes	AT+BSNP used to configure this parameter.
Minimum interval	0x0100	Yes	AT+BSNP used to configure this parameter.
Attempt	0x0008	Yes	AT+BSNP used to configure this parameter.
Timeout	0x0008	Yes	AT+BSNP used to configure this parameter.

The peer device must support and enable sniff mode for it to be operable.

6.6 Park Mode

The firmware does not support park mode. Sniff mode may be used instead if low power operation is required.

6.7 Hold Mode

Parameter	Default	Configurable	Comments
Maximum interval	0x0100	Yes	AT+BSHP used to configure this parameter.
Minimum interval	0x0100	Yes	AT+BSHP used to configure this parameter.

The peer device must support and enable hold mode for it to be operable.

6.8 Device Local Name

Parameter	Default	Configurable	Comments
Local name	“Alps AG”	Yes	AT+BNAM used to configure this parameter.

6.9 Class Of Device

Parameter	Default	Configurable	Comments
Class of Device	0x522204	Yes	AT+BSCD used to configure this parameter.

6.10 Timers

Parameter	Default	Configurable	Comments
Watchdog timeout	3000ms	No	
Watchdog period	500ms	No	
UART recovery timeout	10s	Yes	AT+BURI used to configure this parameter.

6.11 RFCOMM

Parameter	Default	Configurable	Comments
Flow control	Credit based	No	All Bluetooth version 1.1 devices must support RFCOMM credit based flow control.
Maximum Frame Size (MFS)	320bytes	Yes	AT+BMFS used to configure this parameter.

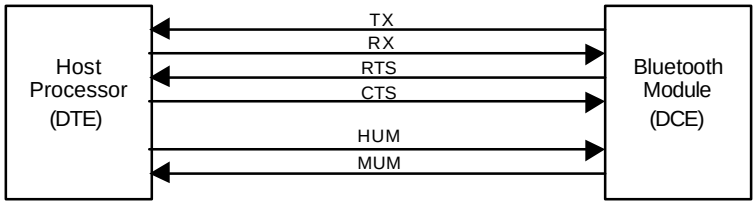
6.12 Bluetooth Supported Features

Parameter	Default	Configurable	Comments
3-slot packets	Supported	No	
5-slot packets	Supported	No	
Encryption	Supported	No	
Slot offset	Supported	No	
Timing accuracy	Supported	No	
Role switch	Supported	No	
Hold mode	Supported	No	
Sniff mode	Supported	No	
Park mode	Not supported	No	Use hold or sniff mode for low power operation if required.
RSSI	Supported	No	
Channel quality driven data rate	Supported	No	
SCO link	Supported	No	
HV2 packets	Supported	No	
HV3 packets	Supported	No	
u-law log	Not supported	No	Custom support possible if required.
A-law log	Not supported	No	Custom support possible if required.
CVSD	Supported	No	
Paging scheme	Supported	No	
Power control	Supported	No	
Transparent SCO data	Not supported	No	Custom support possible if required.
Flow control lag	Not supported	No	

7 Host Interface

7.1 UART Data Discrimination

The firmware uses 2 extra lines in addition to the standard UART lines to differentiate data information and command/result code information. The lines are called *HUM* and *MUM* meaning Host UART Mode and Module UART Mode respectively. The purpose is similar to that of escape sequences that are used to switch between online data state and online command state when controlling modems.
Hardware flow control is highly recommended for applications that require *reliable* data transfer. Without hardware flow control, UART buffer overruns are highly probably and data loss will occur.



7.2 UART Physical Specification

Data and commands are transferred between the host and the module via UART. The Bluetooth module takes the role of the Data Circuit terminating Equipment (DCE) and the host processor takes the roles of the Data Terminal Equipment (DTE). The module's default UART settings are specified below.

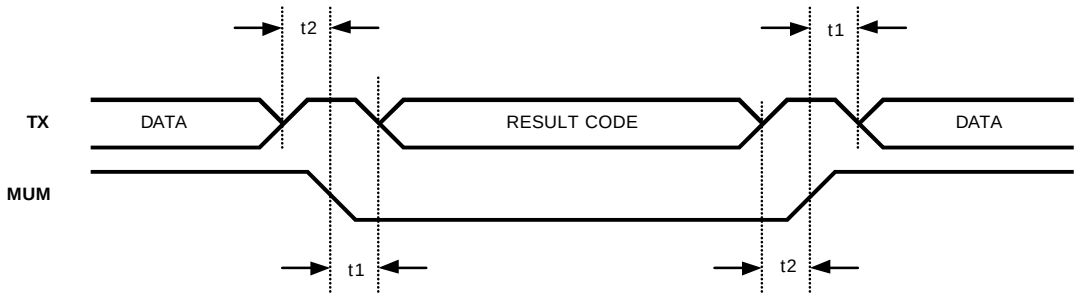
Parameter	Default	Configurable	Comments
Physical Interface	UART	No	
Transport Protocol	None	No	
Baud Rate	115.2kbps	Yes	AT+BURT used to configure this parameter.
Hardware Flow	On	No	Hardware flow control is essential for applications that require reliable transmission of data.
Data bits	8	No	
Stop bits	1	Yes	AT+BURT used to configure this parameter.
Parity	None	Yes	AT+BURT used to configure this parameter.

While it is not possible for the user to configure the UART flow control, it is possible to do so during module production. However, it is essential for hardware flow control to be enabled for applications that require *reliable* transmission of data. Failure to do so may cause UART buffer overflow on the module and therefore loss of data. The UART interface signals used are summarized in the table below. The direction field values should be considered from the Bluetooth module end.

Signal Name	Meaning	Mandatory	Direction	Function
TX	Transmit	Yes	Output	Data transmit
RX	Receive	Yes	Input	Data receive
RTS	Ready To Send	No	Output	Used by module to flow control host.
CTS	Clear To Send	No	Input	Used by host to flow control module.
HUM	Host UART Mode	Yes	Input	Determines if information from host is command (logic 0) or data (logic 1).
MUM	Module UART Mode	Yes	Output	Determines if information from module is result code (logic 0) or data (logic 1).

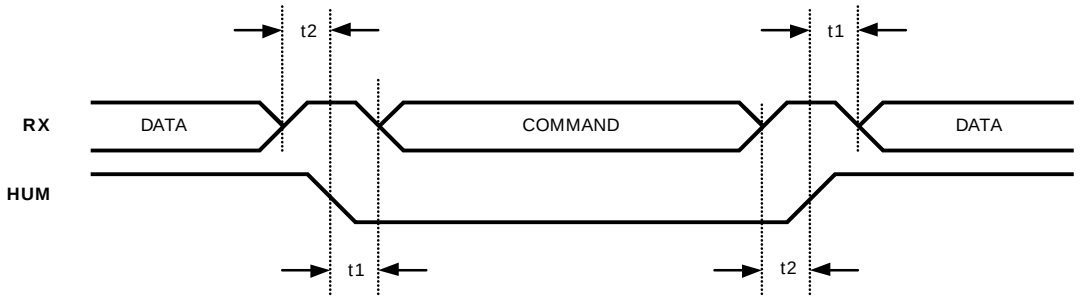
The diagram below gives the timing for data (user data and result code) transmitted from the Bluetooth module to the host processor. Timing is independent of the UART baudrate and other settings. The data setup time and hold times are defined as follows:

Setup time t1 : min 50ms
Hold time t2 : min 50ms



The diagram below gives the timing for data (user data and command) transmitted from the host to the Bluetooth module. The Bluetooth module should not expect more than one command within one HUM pulse. Timing is independent of the UART baudrate and other settings. The data setup time and hold times are defined as follows:

Setup time t1 : min 50ms
Hold time t2 : min 50ms



7.3 UART Logical Specification

The firmware is controlled by way of AT commands similar to those used to control Hayes compatible modems. In response to the AT commands the module generates information responses and result codes. All commands, responses and codes are represented using printable ASCII byte codes. *Ref[2]* gives details of the commands and codes available.

When a Bluetooth connection has been established for the purpose of data transfer, using SPP or DUN for instance, user data should be considered prone to errors. This means that an error recovery mechanism may be required at the transfer application level. The ZModem file transfer protocol uses such an error recovery mechanism.

7.4 UART Configuration

It is possible to configure the module UART settings using the *AT+BURT* command. The new UART settings become effective as soon as the command is parsed and the *OK* result code is sent to the host (using the old UART settings). The new UART settings are stored in flash ROM to be used every time the module is started from that point onwards. The UART parameters are boundary checked but it is still possible to configure the UART in such a way that communication becomes impossible with the host.

To counteract such a problem the firmware contains a mechanism whereby the original default UART settings can be restored and communication made possible again. Similar to the self-configuration feature, when the module boots a UART recovery timer is started if it has been enabled. If no data is sent from the host to the module via the UART before the timer expires, the original default UART settings will be restored. When the UART settings have been recovered, it will be indicated to the host using the *+BURT* unsolicited result code at the recovered UART settings of course. The UART recovery timer is configured using the *AT+BURI* command where a parameter of zero will disable the feature. For added protection, if the UART recovery timer has been disabled, it will not be possible to configure the UART settings using the *AT+BURT* command.

The procedure to configure the UART settings is outlined in the following table:

Command	Result Code	UART Setting	Comment
	READY	115200 8-N-1	Module ready to receive AT commands
AT+BURT=3B0,0,0		115200 8-N-1	Configure UART settings
	OK	115200 8-N-1	Command parsed successfully
+BURT:3B0,0,0		230400 8-N-1	New UART settings

8 Security Policy

The firmware can be configured to use different Security Modes, meeting the requirements of the target application. The available Security Modes and the AT command used to configure them are shown in the table below.

Security Mode	Required AT Command	Comments
Non-secure	AT+BSEC=0	The local device does not enforce any security procedures but will accept any requests from the remote device. For DUN profile only, the local device will enforce authentication and encryption at the service level due to the profile requirement.
Link level	AT+BSEC=1	The local device enforces authentication at the link level. That is, authentication using either PIN codes or link keys must occur before the local device will accept ACL connection requests. For DUN profile only, the local device will enforce encryption too at the service level due to the profile requirement.
Link level with encryption	AT+BSEC=2	This is the same as link level security except that encryption is also requested when ACL connections are setup. This provides the greatest form of secure communication.

Security can be completely disabled by first configuring to the non-secure mode *AT+BSEC=0* and then rejecting all link key and PIN code requests from the remote device. It will also be necessary to remove all devices that have been registered with the Security Manager.

9 Test Features

In order to aid functional verification and certification testing, the firmware supports various test features. The available test features are described in the following sections.

9.1 Bluetooth Test Mode

The Bluetooth specification defines a test mode for the support of testing the Bluetooth transmitter and receiver. It is intended mainly for certification/compliance testing of the radio and baseband layer but may be used for regulatory approval or in-production testing also. Refer to Bluetooth Core Specification, volume 1, v 1.1, February 22nd 2001, Part I:1 for further details of the Bluetooth test mode.

The firmware supports the Bluetooth test mode through the *AT+BDUT* command. When this command is issued the firmware will set the inquiry/page scan parameters to their Bluetooth defaults and then enable Device Under Test (DUT) mode. It is the responsibility of the external processor to issue the *AT+BSLV* command to make the module connectable and discoverable. The command flow is as shown below:

Command	Result Code	Comment
	READY	Module ready to receive AT commands
AT+BDUT		Change scan parameters and enable Device Under Test mode
	OK	Command parsed successfully
AT+BSLV		Enable slave mode
	OK	Command parsed successfully

The external processor should not issue any other commands when DUT mode is enabled. Normal operation will resume when the module is reset.

9.2 Link Condition

By reading the Received Signal Strength Indication (RSSI) and the Link Quality, the condition of an active Bluetooth connection can be verified. The commands to read the values can only be sent to the module when an active connection exists. The meanings of the values returned by the module are specified in the following sections.

9.2.1 Received Signal Strength Indication

It is possible to read the RSSI for the currently active Bluetooth connection using the *AT+BRSI* command. This command provokes a *+BRSI* result code that returns a *signed* 8bit integer giving values between –128 and +127. The Bluetooth specification gives the following definitions:

- If the RSSI is within the Golden Receiver Range, the return value is zero.
- If the RSSI is below the Golden Receiver Range lower limit, the return value is a negative value.
- If the RSSI is above the Golden Receiver Range upper limit, the return value is a positive value.

The Golden Receiver Range is the target signal strength at the receiver. If the RSSI reading rises above the Golden Range upper limit, the return parameter will increase one unit for approximately every dB it rises, i.e. if the signal is 15dB above the golden range then the RSSI value will return +15 (or something close). The value will limit somewhere between +20 and +30: the exact figure depends on the module design. If the RSSI drops below the Golden Range lower limit, the module cannot measure accurately enough to indicate exactly how far the incoming signal strength is below the limit. Instead, the value will vary between –1 and –10 based on how many of the last few packets were below the limit. The measurement will normally limit at –10 or recover to 0 very quickly, without spending much time at the intervening values.
Note that the RSSI return value may be ideal (zero) when either the devices are far apart transmitting at maximum power with RSSI at the bottom of the Golden Range, or very close but transmitting at minimum power with RSSI at the top of the Golden Range. This means that in a power-controlled link the RSSI cannot be used to determine the distance between two Bluetooth devices.

9.2.2 Link Quality

It is possible to read the link quality of the currently active Bluetooth connection using the *AT+BQAL* command. This command provokes a *+BQAL* result code that returns an *unsigned* 8bit integer giving values between 0 and +255. The link quality value is directly related to the Bit Error Rate (BER) with a scale as follows:

Link Quality	BER (%)	Comments
255	0.000	BER resolution between 255 and 215 is 0.0025%.
254	0.0025	
253	0.0050	
…	…	…
215	0.1000	BER resolution between 215 and 89 is 0.0800%.
214	0.1800	0.1800
213	0.2600	0.2600
…	…	…
89	10.1800	BER resolution between 89 and 0 is 0.6400%.
88	10.8200	
87	11.4600	
…	…	…
0	67.1400	

Generally speaking, a link with a BER of between 0% and 0.1% is workable. A link with a BER above 1% will give poor results. The scale below 215 is not fully characterized since results in this region are not stable and often indicate that a link is dropping more packets than it is receiving.

10 Persistent Store

The Bluetooth module contains flash ROM that is used to persistently store, amongst other things, configuration data for the firmware. The block of flash ROM allocated for the configuration data is called Persistent Store (PS). Through the use of AT commands it is possible for an external processor to change various firmware configuration values and store these in PS to be used as the default values every time the module is powered up or is reset.

The flash ROM imposes certain limitations that affect the way in which new parameter values are stored. Individual entries cannot be erased or overwritten so when a parameter is changed and stored in PS the old value is marked as unused and the new value is appended to the end of the PS memory block. This means that as changes are made to the parameters, the amount of memory available for PS decreases. There is a finite amount of memory allocated for PS so if many changes are carried out, it will fill up and further changes will not be possible.

When the module powers up or is reset, it reads all necessary configuration data from the PS. This can be a time consuming process and will therefore account for a large percentage of the firmware boot time. It follows that as the amount of PS utilized increases, so does the boot time.

The following AT commands can cause changes to be made to the PS:

Command	Description
AT+BNAM=<name>	Change the Local Name
AT+BURT=<rate>,<stop>,<parity>	Change UART settings
AT+BURI=<time>	Change UART recover timer

In order to get around the problems associated with PS, the firmware will attempt to remove all of the redundant data from the PS leaving only the newest values of each parameter. This clean-up process is known is defrag. Note that the boot time when defrag is performed is substantially longer than usual. The firmware can automatically defrag the PS or an external processor can request the firmware to perform the defrag explicitly using an AT command.

10.1 Automatic Defrag

When the PS utilization reaches 70%, the firmware will automatically perform the defrag when it next boots up. It is possible for the PS to reach 100% if changes are made to the PS without the resetting the module or powering it down and then up again. Excluding when a defrag occurs, the longest boot time will be experienced when the PS utilization is just below the 70% threshold.

It is important to note that the module power supply must remain constant during the defrag process in order to maintain the integrity of the contents of PS.

10.2 Forced Defrag

It is not possible to directly configure the 70% threshold figure used for automatic defrag. However, an external processor can read the current utilization from the firmware and force a defrag based on that value. The *AT+BDFG?* command is used to read the current PS utilization defined as a percentage of the total PS available. The *AT+BDFG* command is used to force the defrag itself. In order for the defrag to occur the module must reboot and this handled automatically by the firmware.

It is important to note that the module power supply must remain constant during the defrag process in order to maintain the integrity of the contents of PS.

An example command sequence follows where the external processor has determined that a threshold of 50% is necessary for the intended application.

Command	Result Code	Comment
	READY	Module ready to receive AT commands
AT+BDFG?	OK	Read current PS utilization command parsed successfully
	+BDFG:54	Current PS utilization is approximately 54%
AT+BDFG	OK	Forces defrag command parsed successfully.
	READY	Defrag complete, module ready to receive AT commands

11 Programmable Input / Output

HUM **Host UART Mode**
This input PIO is used to determine if the information received from the host is user data or AT commands. A logic '1' indicates data and a logic '0' indicates AT command.

MUM **Module UART Mode**
This output PIO is used to determine if the information sent to the host is user data or a result code. A logic '1' indicates data and a logic '0' indicates result code.

UGXZ2 (Version2 Class2 SMD)

Port Name	Pin	Direction	Name	Function
PIO[2] / PORT4	10	Input	HUM	Determines the type of information received via UART.
PIO[4] / PORT3	9	Output	MUM	Determines the type of information transmitted via UART.

UGPZ1 (Version2 Class1 FIT)

Port Name	Pin	Direction	Name	Function
PIO[2] / Port2	4	Input	HUM	Determines the type of information received via UART.
PIO[7] / LED/FlashPort2	19	Output	MUM	Determines the type of information transmitted via UART.

12 Known Issues / Outstanding Items

- The current version of this firmware will always connect to the 1st instance of a particular profile found on the remote device. This means that if the remote slave has more than one instance of the same profile, for example 3 SPP instances, it is not possible to connect to the 2nd or 3rd instance.

13 References

In the following references *xxx* is the firmware version and *yy* is the document version.

Ref[1]	Alps_VCL_USER_*xxx_yy*.pdf	Users Guide
Ref[2]	AlpsVCL_AT_*xxx_yy*.pdf	AT Command Reference List

14 Document Change History

14.1 Alpha Version

Version	Section	Details
Alpha4 1.1	Host Interface – Physical	Corrected signal directions in table and in diagram.
Alpha4 1.2	All	Formatting changes for addition of Contents section.
Alpha5 1.0	Host Interface	Created one main section and added sub-section detailing the user UART configuration feature.
Alpha6 1.0	Programmable I/O	Corrected mistake in MUM description. Input Ÿ Output.
Alpha6 1.0	UART Physical Specification	Added detailed timing charts and descriptions. Removed previous waveform diagram.
Alpha6 1.0	Host Interface	Changed sub-section ordering.
Alpha7 1.0	Functionality	Changed service attributes as dynamic registration is implemented.
Alpha7 1.0	Functionality	Updated profile descriptions to make it clear that DUN and FAX profiles are hosted i.e. applications reside on host processor.

14.2 Beta Version

Version	Section	Details
Beta2 1.0	Functionality	Removed Fax Profile Hosting sub-section.
Beta2 1.0	Host Interface	Removed UART Configuration sub-section.
Beta2 1.1	RSSI Return Value	Added new section.
Beta2 1.1	Link Quality Return Value	Added new section.
Beta2 1.2	Functionality	Changed descriptions of Hands-Free Profile sub-section.
Beta2 1.3	State Diagram	Add new section.
Beta3 1.0	Functionality	Changed description of Hands-Free Profile sub-section due to supported HFP adopted version 1.0.
Beta3 1.0	Functionality	Described service records more detail.
Beta3 1.0	Functionality	Integrated State Diagram section into Test Features section.
Beta3 1.0	System Configuration	Added new section.
Beta3 1.0	Host Interface	Added the UART recovery timer description.
Beta3 1.0	Security Policy	Added new section.
Beta3 1.0	Test Features	Added new section.
Beta3 1.0	Test Features	Integrated RSSI Return Value and Link Quality Return Value sections into Test Features section.
Beta3 1.0	Persistent Store	Added new section.
Beta3 1.0	Programmable Input / Output	Added the pin assignment for UGPZ1 module.
Beta3 1.0	Test Results	Added new section.

14.3 Official Version

Version	Section	Details
Revision B3_10	All	First Release

15 Test Results

15.1 AT Command tests

Command Sequence	Iterations	Result	Comments
AT+BSLV	100	Pass	Success check
AT+BMST=0,2,C7,A10002	100	Pass	Success check
AT+BMST=0,2,C7,11A10002	100	Pass	Failure check
AT+BDIS	100	Pass	Success check
AT+BACN=1	100	Pass	Success check
AT+BACN=0	100	Pass	Failure check
AT+BADS	100	Pass	Success check
AT+BINQ=0,0,5,A	100	Pass	Success check
AT+BINQ=0,0,B,A	100	Pass	Failure check
AT+BRSI	100	Pass	Success check
AT+BQAL	100	Pass	Success check
AT+BMSC=B,0	100	Pass	Success check
AT+BMSC=20,0	100	Pass	Failure check
AT+BESM	100	Pass	Success check
AT+BXSM	100	Pass	Success check
AT+BEHM	100	Pass	Success check
AT+BSEC=1	100	Pass	Success check
AT+BSEC=3	100	Pass	Failure check
AT+BSEC?	100	Pass	Success check
AT+BPIN=	100	Pass	Success check
AT+BPIN=1234	100	Pass	Success check
AT+BPIN=12345678901234567	100	Pass	Failure check
AT+BLNK=	100	Pass	Success check
AT+BLNK=12345678901234567890123456789012	100	Pass	Success check
AT+BLNK=1234	100	Pass	Failure check
AT+BSDA=2,C7,A10002,12345678901234567890123456789012	100	Pass	Success check
AT+BSDA=2,C7,A10002,1234	100	Pass	Failure check
AT+BSDD=2,C7,A10002	100	Pass	Success check
AT+BSDD=2,C7,11A10002	100	Pass	Failure check
AT+BRNG=	100	Pass	Success check
AT+BRNG=0244365111	100	Pass	Success check
AT+BCUS=AT+BADD	100	Pass	Success check
AT+BVGS=7	100	Pass	Success check
AT+BVGS=10	100	Pass	Failure check
AT+BVGM=7	100	Pass	Success check
AT+BVGM=10	100	Pass	Failure check
AT+BSIR=1	100	Pass	Success check
AT+BSIR=2	100	Pass	Failure check
AT+BVRA=1	100	Pass	Success check
AT+BVRA=2	100	Pass	Failure check
AT+BINP=	100	Pass	Success check
AT+BINP=0244365111	100	Pass	Success check
AT+BCWN=0244365111	100	Pass	Success check
AT+BIES=1	100	Pass	Success check
AT+BIES=2	100	Pass	Failure check
AT+BIEC=1	100	Pass	Success check
AT+BIEC=2	100	Pass	Failure check
AT+BIEP=1	100	Pass	Success check
AT+BIEP=4	100	Pass	Failure check
AT+BCNL	100	Pass	Success check
AT+BNAM=12345678901234567890123456789012 AT+BNAM=01234567890123456789012345678901	100	Pass	Success check
AT+BNAM=12345678901234567890123456789012	100	Pass	Failure check
AT+BRSR=1,0	100	Pass	Success check
AT+BRSR=20,FF000000	100	Pass	Failure check
AT+BSSP=800,12,800,12	100	Pass	Success check
AT+BSSP=1800,12,800,12	100	Pass	Failure check
AT+BSSP?	100	Pass	Success check
AT+BSNP=160,160,8,8	100	Pass	Success check
AT+BSNP=160,160,0,0	100	Pass	Failure check
AT+BSNP?	100	Pass	Success check
AT+BSHP=160,160	100	Pass	Success check
AT+BSHP=160,0	100	Pass	Failure check
AT+BSHP?	100	Pass	Success check
AT+BWLP=6	100	Pass	Success check
AT+BWLP=8	100	Pass	Failure check
AT+BWLP?	100	Pass	Success check
AT+BSCD=522204	100	Pass	Success check
AT+BSCD=1FFFFFF	100	Pass	Failure check
AT+BSCD?	100	Pass	Success check

AT+BMFS=64	100	Pass	Success check
AT+BMFS=2BD	100	Pass	Failure check
AT+BMFS?	100	Pass	Success check
AT+BDUT	100	Pass	Success check
AT+BRST	100	Pass	Success check
AT+BECO=0	100	Pass	Success check
AT+BECO=2	100	Pass	Failure check
AT+BECO?	100	Pass	Success check
AT+BEVT=2	100	Pass	Success check
AT+BEVT=3	100	Pass	Failure check
AT+BEVT?	100	Pass	Success check
AT+BURT=1D8,0,0	100	Pass	Success check
AT+BURT=1D8,0,4	100	Pass	Failure check
AT+BURI=1	100	Pass	Success check
AT+BURI=200	100	Pass	Failure check
AT+BURI?	100	Pass	Success check
AT+BTUN=1	100	Pass	Success check
AT+BTUN=2	100	Pass	Failure check
AT+BTUN?	100	Pass	Success check
AT+BDFG	100	Pass	Success check
AT+BDFG?	100	Pass	Success check

15.2 AT Command parameter boundary tests

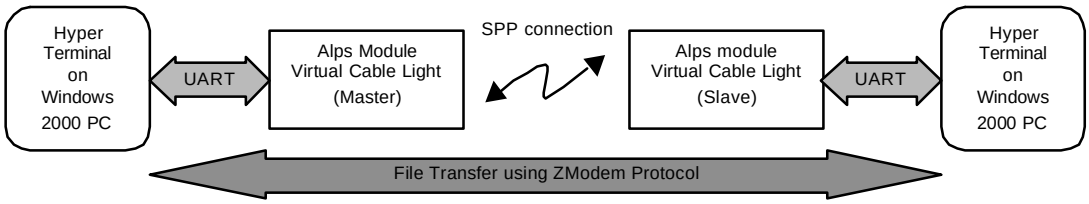
Command	Parameter	Result	Comments
AT+BMST	0,0,0,0	Pass	Success check
	3,0,0,0	Pass	Success check
	5,FFFF,FF,FFFFFF	Pass	Success check
	1,0,0,0	Pass	Failure check
	2,0,0,0	Pass	Failure check
	6,0,0,0	Pass	Failure check
	0,10000,0,0	Pass	Failure check
	0,0,100,0	Pass	Failure check
	0,0,0,1000000	Pass	Failure check
AT+BACN	1	Pass	Success check
	3	Pass	Success check
	0	Pass	Failure check
	4	Pass	Failure check
AT+BINQ	0,0,1,2	Pass	Success check
	FFFFFF,FFFFFF,A,3C	Pass	Success check
	1000000,0,1,2	Pass	Failure check
	0,1000000,1,2	Pass	Failure check
	0,0,B,2	Pass	Failure check
	0,0,1,3D	Pass	Failure check
AT+BMSC	0,0	Pass	Success check
	1F,FF	Pass	Success check
	20,0	Pass	Failure check
	0,100	Pass	Failure check
AT+BSEC	0	Pass	Success check
	2	Pass	Failure check
	3	Pass	Failure check
AT+BPIN		Pass	Success check
	1234567890123456	Pass	Success check
	12345678901234567	Pass	Failure check
AT+BLNK		Pass	Success check
	123456789012345678901234567890123	Pass	Success check
	1	Pass	Failure check
	12345678901234567890123456789012	Pass	Failure check
	123456789012345678901234567890123	Pass	Failure check
AT+BSDA	0,0,0,123456789012345678901234567890123	Pass	Success check
	FFFF,FF,FFFFFF,123456789012345678901234567890123	Pass	Success check
	10000,0,0,123456789012345678901234567890123	Pass	Failure check
	0,100,0,123456789012345678901234567890123	Pass	Failure check
	0,0,1000000,123456789012345678901234567890123	Pass	Failure check
	0,0,0,12345678901234567890123456789012	Pass	Failure check
	0,0,0,123456789012345678901234567890123	Pass	Failure check
AT+BSDD	0,0,0	Pass	Success check
	FFFF,FF,FFFFFF	Pass	Success check
	10000,0,0	Pass	Failure check
	0,100,0	Pass	Failure check
	0,0,1000000	Pass	Failure check
AT+BVGS	0	Pass	Success check
	F	Pass	Success check
	10	Pass	Failure check
AT+BVGM	0	Pass	Success check
	F	Pass	Success check
	10	Pass	Failure check
AT+BSIR	0	Pass	Success check
	1	Pass	Success check
	2	Pass	Failure check
AT+BVRA	0	Pass	Success check
	1	Pass	Success check
	2	Pass	Failure check
AT+BIES	0	Pass	Success check
	1	Pass	Success check
	2	Pass	Failure check
AT+BIEC	0	Pass	Success check
	1	Pass	Success check
	2	Pass	Failure check
AT+BIEP	0	Pass	Success check
	3	Pass	Success check
	4	Pass	Failure check
AT+BNAM		Pass	Success check
	1234567890123456789012345678901	Pass	Success check
	123456789012345678901234567890123	Pass	Failure check
AT+BRSR	1,0	Pass	Success check
	3B,3F3F0001	Pass	Success check
	0,0	Pass	Failure check

	3C,3F3F0001	Pass	Failure check
	3B,3F3F0002	Pass	Failure check
AT+BSSP	0,0,0,0	Pass	Success check
	12,12,12,12	Pass	Success check
	1000,1000,1000,1000	Pass	Success check
	11,12,12,12	Pass	Failure check
	1001,12,12,12	Pass	Failure check
	12,11,12,12	Pass	Failure check
	12,1001,12,12	Pass	Failure check
	12,12,11,12	Pass	Failure check
	12,12,1001,12	Pass	Failure check
	12,12,12,11	Pass	Failure check
	12,12,12,1001	Pass	Failure check
	12,13,12,12	Pass	Failure check
	12,12,12,13	Pass	Failure check
	12,0,12,12	Pass	Failure check
	12,12,12,0	Pass	Failure check
AT+BSNP	1,1,1,0	Pass	Success check
	FFFF,FFFF,7FFF,7FFF	Pass	Success check
	0,1,1,0	Pass	Failure check
	10000,1,1,0	Pass	Failure check
	1,0,1,0	Pass	Failure check
	1,10000,1,0	Pass	Failure check
	1,1,0,0	Pass	Failure check
	1,1,8000,0	Pass	Failure check
	1,1,1,8000	Pass	Failure check
	1,2,1,0	Pass	Failure check
AT+BSHP	1,1	Pass	Success check
	FFFF,FFFF	Pass	Success check
	0,1	Pass	Failure check
	10000,1	Pass	Failure check
	1,0	Pass	Failure check
	1,10000	Pass	Failure check
	1,2	Pass	Failure check
AT+BWLP	0	Pass	Success check
	7	Pass	Success check
	8	Pass	Failure check
AT+BSCD	0	Pass	Success check
	FFFFFF	Pass	Success check
	1000000	Pass	Failure check
AT+BMFS	2C	Pass	Success check
	2BC	Pass	Success check
	2B	Pass	Failure check
	2BD	Pass	Failure check
AT+BECO	0	Pass	Success check
	1	Pass	Success check
	2	Pass	Failure check
AT+BEVT	0	Pass	Success check
	2	Pass	Success check
	3	Pass	Failure check
AT+BURT	0,0,0	Pass	Success check
	EBF,2,3	Pass	Success check
	EC0,0,0	Pass	Failure check
	0,3,0	Pass	Failure check
	0,0,4	Pass	Failure check
AT+BURI	0	Pass	Success check
	12C	Pass	Success check
	12D	Pass	Failure check
AT+BTUN	0	Pass	Success check
	1	Pass	Success check
	2	Pass	Failure check

15.3 Bulk File Transfer

15.3.1 Test Conditions

Remote Device	
Hardware	Alps CL2 UGXZ2
Bluetooth protocol stack	Alps Virtua Cable Light
File transfer application	HyperTerminal on Windows 2000 using ZModem transfer protocol
Local Device	
UART Baud Rate	115200bps
UART Data Bits	8bit
UART Stop Bits	1bit
UART Parity	None
UART tuning	Throughput
File transfer application	HyperTerminal on Windows 2000 using ZModem transfer protocol
Data	
File size	100MB
File contents	Binary data
Miscellaneous	
RFCOMM Maximum Frame Size	320 bytes
Link Condition	RSSI = 0, Link Quality = 255



15.3.2 Test Results

The test result is a pass if the complete data file is received with no retransmissions.

File Transfer Direction	Iterations	Result	Comments
Master to Slave	2	Pass	Half duplex transfer
Slave to Master	2	Pass	Half duplex transfer

15.4 Functional tests

15.4.1 Establish and Release Service Connection

No	Command	Possible Response(s)	Comments
1	AT+BRSR=1,0	OK +BRSR	Register the SPP service.
2	AT+BMST=0,2,C7,A10002	OK +BMSC:0,0 +BRFC:2,C7,A10002,0,0,0	Connect as master.
3	-	+BRFC:0,0,0,FFFF,3,0	Initiate SPP disconnection from the remote device.
4	AT+BSLV	OK +BMSC:0,0 +BRFC:2,C7,A10002,0,0,0	Connect as slave.
5	AT+BDIS	OK +BRFC:0,0,0,FFFF,3,0	Initiate SPP disconnection from the local device.
6	-	-	Iterate 100 times from 2 to 5.

15.4.2 Inquiry

No	Command	Possible Response(s)	Comments
1	AT+BINQ=0,0,5,A	OK +BINQ:2,C7,EE0078,2104,NetVista +BINQ:2,C7,A10002,522204,AG02 +BINC:1	Perform an inquiry for all device types.
2	-	-	Iterate 100 times.

15.4.3 Establish and Release SCO Connection

No	Command	Possible Response(s)	Comments
1	AT+BRSR=1,0	OK +BRSR	Register the SPP service.
2	AT+BMST=0,2,C7,A10002	OK +BMSC:0,0 +BRFC:2,C7,A10002,0,0,0	Connect as master.
3	-	+BSCO:0	Establish SCO connection from remote device.
4	AT+BADS	OK +BSCO:3	Initiate SCO disconnection from the local device.
5	AT+BACN=1	OK +BSCO:0	Establish SCO connection from the local device.
6	-	+BSCO:3	Initiate SCO disconnection from the remote device.
7	-	-	Iterate 100 times from 3 to 6.
8	AT+BDIS	OK +BRFC:0,0,0,FFFF,3,0	Initiate SPP disconnection from the local device.

15.4.4 Register/Unregister a Remote Device to/from the Security Database

No	Command	Possible Response(s)	Comments
1	AT+BSDA=2,C7,A10002,E8A3DFD672 7EC08B7737044E93FF1634	OK	Add a peer device to the security database with link key.
2	AT+BSDD=2,C7,A10002	OK	Delete the registered device from the security database.
3	-	-	Iterate 100 times from 1 to 2.

15.4.5 Pair with Remote Device

No	Command	Possible Response(s)	Comments
1	AT+BRSR=1,0	OK +BRSR	Register the SPP service.
2	AT+BSEC=2	OK	Set security to mode 3 with encryption.
3	AT+BMST=0,2,C7,A10002	OK +BLNK:2,C7,A10002	Connect as master.
4	AT+BLNK=	OK +BPIN:2,C7,A10002	Reject the link key request.
5	AT+BPIN=1522	OK +BPRC:2,C7,A10002,72458310288CE6 31454F47214A5BD646 +BMSC:0,0 +BRFC:2,C7,A10002,0,0,0	Accept the PIN code request with a PIN code “1522”.
6	-	+BRFC:0,0,0,FFFF,3,0	Initiate SPP disconnection from the remote device.
7	AT+BSDD=2,C7,A10002	OK	Delete the registered device from the security database.
8	AT+BSLV	OK	Connect as slave.

		+BLNK:2,C7,A10002	
9	AT+BLNK=	OK +BPIN:2,C7,A10002	Reject the link key request.
10	AT+BPIN=1522	OK +BPRC:2,C7,A10002,7F0E8762F9358EDF339285C5039484AA +BMSC:0,0 +BRFC:2,C7,A10002,0,0,0	Accept the PIN code request with a PIN code "1522". Pairing success when the local PIN code and the remote PIN code are the same.
11	AT+BDIS	OK +BRFC:0,0,0,FFFF,3,0	Initiate SPP disconnection from the local device.
12	AT+BSDD=2,C7,A10002	OK	Delete the registered device from the security database.
13	-	-	Iterate 100 times from 3 to 12.

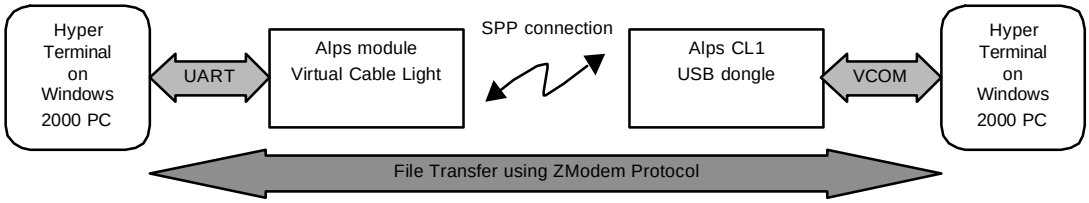
15.4.6 Low Power Modes

No	Command	Possible Response(s)	Comments
1	AT+BRSR=1,0	OK +BRSR	Register the SPP service.
2	AT+BWLP=6	OK	Set the default link policy settings to enable hold/sniff mode.
3	AT+BSHP=FFFF,1000	OK	Set the hold mode parameters.
4	AT+BSNP=2000,1000,100,10	OK	Set the sniff mode parameters.
5	AT+BMST=0,2,C7,A10002	OK +BMSC:0,0 +BRFC:2,C7,A10002,0,0,0	Connect as master.
6	AT+BEHM	OK +BCHM:1,1E50	Enter hold mode from the local device.
7	-	+BCHM:0,0	Connection returns to active mode.
8	-	+BCHM:1,1E50	Enter hold mode from the remote device.
9	-	+BCHM:0,0	Connection returns to active mode.
10	AT+BESM	OK +BCHM:2,2000	Enter the sniff mode from the local device.
11	-	+BCHM:0,0	Exit the sniff mode from the remote device.
12	-	+BCHM:2,2000	Enter the sniff mode from the remote device.
13	AT+BXSM	OK +BCHM:0,0	Exit the sniff mode from the local device.
14	-	-	Iterate 100 times from 6 to 13.
15	AT+BDIS	OK +BRFC:0,0,0,FFFF,3,0	Initiate SPP disconnection from the local device.

15.5 Throughput Measurement

15.5.1 Test Conditions

Remote Device	
Hardware	Alps CL1 USB dongle, firmware version 14.6
Bluetooth protocol stack	IVT BlueSoleil BTP-1.0.7 / 04.00.00.0724
File transfer application	HyperTerminal on Windows 2000 using ZModem transfer protocol
Local Device	
UART Baud Rate	115200bps / 230400bps / 460800bps
UART Data Bits	8bit
UART Stop Bits	1bit
UART Parity	None
UART tuning	Throughput / Latency
File transfer application	HyperTerminal on Windows 2000 using ZModem transfer protocol
Data	
File size	100MB
File contents	Binary data
Miscellaneous	
RFCOMM Maximum Frame Size	44 bytes / 320 bytes / 700 bytes
Link Condition	RSSI = 0, Link Quality = 255



15.5.2 Test Results

The throughput was calculated by noting the time that it took HyperTerminal to send the file, not the throughput reported by HyperTerminal. The calculated throughput value will still include overhead and compression employed by the ZModem protocol. The following results were measured when the UART was tuned for throughput.

Baudrate [bps]	AG Role	File Transfer Direction	MFS [bytes]	Throughput [bps]
115200	Master	Alps VCL to Alps USB dongle	44	17,735
			320	90,200
			700	90,200
		Alps USB dongle to Alps VCL	44	41,323
			320	88,301
			700	89,241
	Slave	Alps VCL to Alps USB dongle	44	12,210
			320	43,240
			700	90,200
		Alps USB dongle to Alps VCL	44	20,165
			320	89,241
			700	89,241
230400	Master	Alps VCL to Alps USB dongle	44	19,329
			320	71,698
			700	171,196
		Alps USB dongle to Alps VCL	44	41,121
			320	144,631
			700	142,180
	Slave	Alps VCL to Alps USB dongle	44	13,443
			320	48,489
			700	73,584
		Alps USB dongle to Alps VCL	44	20,165
			320	93,207
			700	119,837
460800	Master	Alps VCL to Alps USB dongle	44	20,165
			320	67,650
			700	97,542
		Alps USB dongle to Alps VCL	44	41,323
			320	149,797
			700	149,797
	Slave	Alps VCL to Alps USB dongle	44	13,487
			320	64,528
			700	78,398
		Alps USB dongle to Alps VCL	44	20,165
			320	96,421
			700	119,837

The following results were measured when the UART was tuned for latency.

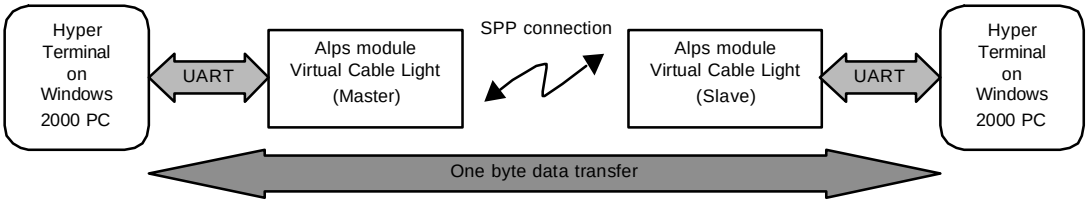
Baudrate [bps]	AG Role	File Transfer Direction	MFS [bytes]	Throughput [bps]
115200	Master	Alps VCL to Alps USB dongle	44	17,476
			320	43,019
			700	68,200
		Alps USB dongle to Alps VCL	44	44,151
			320	90,200
			700	90,200
	Slave	Alps VCL to Alps USB dongle	44	11,798
			320	33,825
			700	52,789
		Alps USB dongle to Alps VCL	44	20,117
			320	86,480
			700	88,301
230400	Master	Alps VCL to Alps USB dongle	44	19,065
			320	69,327
			700	103,563
		Alps USB dongle to Alps VCL	44	41,323
			320	144,631
			700	142,180
	Slave	Alps VCL to Alps USB dongle	44	12,653
			320	48,210
			700	71,698
		Alps USB dongle to Alps VCL	44	20,068
			320	94,254
			700	119,837
460800	Master	Alps VCL to Alps USB dongle	44	20,068
			320	67,109
			700	91,181
		Alps USB dongle to Alps VCL	44	41,323
			320	149,797
			700	149,797
	Slave	Alps VCL to Alps USB dongle	44	13,066
			320	63,550
			700	75,537
		Alps USB dongle to Alps VCL	44	20,117
			320	95,325
			700	119,837

15.6 Latency measurement

Latency was measured as the time for one byte of data to travel from the UART of the sending device to the UART of the receiving device. Note that latency figures for continuous data transfer will tend to differ from those presented here.

15.6.1 Test Conditions

Remote Device	
Hardware	Alps CL2 UGXZ2
Bluetooth protocol stack	Alps Embedded Audio Gateway
Data transfer application	HyperTerminal on Windows 2000
Local Device	
UART Baud Rate	115200bps / 230400bps
UART Data Bits	8bit
UART Stop Bits	1bit
UART Parity	None
UART tuning	Throughput / Latency
File transfer application	HyperTerminal on Windows 2000
Miscellaneous	
RFCOMM Maximum Frame Size	44 bytes / 320 bytes / 700 bytes
Link Condition	RSSI = 0, Link Quality = 255



15.6.2 Test Results

The following results were measured when the UART was tuned for throughput.

Baudrate [bps]	File Transfer Direction	MFS [bytes]	Latency [ms]												
			1	2	3	4	5	6	7	8	9	10	Max	Min	Ave
115200	Master to Slave	44	24.4	24.4	27.2	28.6	39.0	37.4	26.8	23.6	34.0	32.0	39.0	23.6	29.74
		320	23.0	36.0	26.0	38.8	37.2	31.2	32.6	24.8	33.2	29.8	38.8	23.0	31.26
		700	26.0	24.2	37.2	25.0	26.8	38.2	31.2	44.0	40.2	35.2	44.0	24.2	32.80
	Slave to Master	44	43.4	50.4	37.6	56.8	49.2	39.6	37.0	52.4	39.8	44.6	56.8	37.0	45.08
		320	51.0	38.6	44.2	43.6	51.4	47.4	57.0	44.8	44.8	36.2	57.0	36.2	45.90
		700	46.6	53.4	37.0	41.2	52.6	41.6	54.6	50.6	36.8	51.6	54.6	36.8	46.60
230400	Master to Slave	44	27.8	39.4	25.6	40.2	26.4	30.0	27.4	39.2	26.6	27.4	40.2	25.6	31.00
		320	25.6	28.0	35.2	27.6	33.4	29.2	39.2	23.6	38.8	34.2	39.2	23.6	31.48
		700	40.2	32.0	24.8	24.6	41.4	43.2	39.8	26.0	37.8	35.0	43.2	24.6	34.48
	Slave to Master	44	46.8	50.4	45.0	51.8	40.2	37.6	48.0	37.2	42.0	49.4	51.8	37.2	44.84
		320	45.2	50.6	45.4	45.0	46.6	38.8	44.8	47.0	58.2	41.6	58.2	38.8	46.32
		700	47.8	65.2	54.8	44.0	48.8	39.4	42.0	45.4	49.6	39.0	65.2	39.0	47.60

The following results were measured when the UART was tuned for latency.

Baudrate [bps]	File Transfer Direction	MFS [bytes]	Latency [ms]												
			1	2	3	4	5	6	7	8	9	10	Max	Min	Ave
115200	Master to Slave	44	24.4	29.8	27.4	23.4	39.2	24.8	30.0	36.0	29.6	24.8	39.2	23.4	28.94
		320	35.0	22.8	30.6	27.6	26.6	37.0	40.0	23.6	31.2	30.6	40.0	22.8	30.50
		700	37.0	34.4	40.4	38.4	25.8	31.8	28.6	37.2	25.2	27.4	40.4	25.2	32.62
	Slave to Master	44	40.6	49.2	45.6	49.6	39.0	41.2	39.8	52.6	46.2	45.4	52.6	39.0	44.92
		320	39.2	46.6	48.8	37.4	36.6	41.6	56.2	54.2	48.8	46.6	56.2	36.6	45.60
		700	40.6	41.8	38.0	51.4	45.0	50.6	47.2	41.4	49.8	58.6	58.6	38.0	46.44
230400	Master to Slave	44	31.0	35.6	28.6	28.4	32.6	37.6	29.2	29.0	25.8	31.2	37.6	25.8	30.90
		320	25.6	32.0	30.0	27.8	32.0	35.2	28.8	37.0	35.2	25.0	37.0	25.0	30.86
		700	24.2	34.6	30.2	35.4	25.4	43.4	30.4	31.0	41.2	36.6	43.4	24.2	33.24
	Slave to Master	44	44.4	38.4	46.6	37.6	50.0	40.4	44.6	43.2	55.0	53.6	55.0	37.6	45.38
		320	55.6	62.2	41.4	47.0	36.8	48.4	38.4	47.2	53.2	45.0	62.2	36.8	47.52
		700	46.2	51.6	45.2	39.0	43.6	53.0	37.2	51.4	67.2	41.2	67.2	37.2	47.56

15.7 Power consumption (UGXZ2)

15.7.1 Idle State

Extra Details	Current Consumption [mA]				
Host Communication	Max	High	Low	Min	Mean
Inactive	16.64	15.45	2.337	1.678	2.780
Active	16.70	15.65	15.38	14.60	15.39

15.7.2 Inquiring and Paging State

	Current Consumption [mA]				
State	Max	High	Low	Min	Mean
Inquiring	58.75	52.90	47.51	37.03	49.20
Paging	58.77	52.99	47.44	36.95	49.28

15.7.3 Discoverable and Connectable State

Inquiry Scan [ms]		Page Scan [ms]		Current Consumption [mA]				
Interval	Window	Interval	Window	Max	High	Low	Min	Mean
2560	11.25	0	0	61.77	61.36	2.468	1.941	3.094
160	160	0	0	62.17	61.29	15.82	14.76	60.46
0	0	2560	11.25	61.53	61.24	2.382	1.856	3.067
0	0	160	160	61.91	61.24	32.73	32.18	60.57
2560	11.25	2560	11.25	61.82	61.29	2.477	1.950	3.377
160	80	160	80	62.40	61.39	15.58	13.32	59.48
1280	11.25	640	50	62.10	61.45	2.430	1.900	8.088

15.7.4 RFCOMM Connected State

The following results were measured when the role was master.

Sniff Parameters (ms)			Hold Parameters	Extra Details		Current Consumption [mA]				
Interval	Attempt	Timeout	Interval (ms)	Data	Audio	Max	High	Low	Min	Mean
-	-	-	-	No	No	57.06	43.06	2.290	1.803	6.758
-	-	-	-	M Ÿ S	No	57.56	56.21	15.42	9.763	23.53
-	-	-	-	S Ÿ M	No	61.76	58.08	15.38	1.981	25.44
-	-	-	-	No	HV1	61.85	55.74	47.26	39.76	53.18
-	-	-	-	No	HV2	62.19	61.13	16.33	15.37	37.58
-	-	-	-	No	HV3	62.43	58.33	15.85	3.441	29.23
160	9.375	9.375	-	No	No	56.54	41.28	2.380	1.791	4.213
160	9.375	9.375	-	No	HV1	61.96	55.92	47.32	40.43	53.35
160	9.375	9.375	-	No	HV2	62.20	55.67	16.26	15.49	36.43
160	9.375	9.375	-	No	HV3	62.39	61.18	15.85	3.447	28.44
1000	9.375	9.375	-	No	No	56.52	54.87	2.494	1.906	3.208
1000	9.375	9.375	-	No	HV1	61.81	55.72	43.03	24.55	53.20
1000	9.375	9.375	-	No	HV2	62.01	55.47	16.16	15.29	35.97
1000	9.375	9.375	-	No	HV3	62.31	58.34	15.84	3.600	27.89
-	-	-	4000	No	No	16.30	15.49	2.428	1.819	2.828

The following results were measured when the role was slave.

Sniff Parameters (ms)			Hold Parameters	Extra Details		Current Consumption [mA]				
Interval	Attempt	Timeout	Interval (ms)	Data	Audio	Max	High	Low	Min	Mean
-	-	-	-	No	No	56.56	40.74	19.20	16.24	28.37
-	-	-	-	M Ÿ S	No	59.73	58.13	16.64	10.19	32.42
-	-	-	-	S Ÿ M	No	57.50	56.23	16.59	9.606	33.57
-	-	-	-	No	HV1	61.32	58.54	46.76	38.26	52.74
-	-	-	-	No	HV2	61.58	58.78	16.95	16.11	40.80
-	-	-	-	No	HV3	61.74	53.12	18.45	16.08	36.60
160	9.375	9.375	-	No	No	56.85	40.15	2.458	1.975	4.825
160	9.375	9.375	-	No	HV1	61.20	58.51	46.82	38.49	52.68
160	9.375	9.375	-	No	HV2	61.44	58.65	16.45	14.67	35.36
160	9.375	9.375	-	No	HV3	61.61	59.14	16.49	14.02	29.48
1000	9.375	9.375	-	No	No	60.95	55.68	2.359	1.722	3.191
1000	9.375	9.375	-	No	HV1	61.15	58.39	46.79	37.89	52.54
1000	9.375	9.375	-	No	HV2	60.98	57.96	16.50	15.01	34.83
1000	9.375	9.375	-	No	HV3	61.59	59.14	16.59	14.23	28.83
-	-	-	4000	No	No	16.11	15.36	2.366	1.763	2.748

15.8 Power consumption (UGPZ1)

15.8.1 Idle State

Extra Details	Current Consumption [mA]				
Host Communication	Max	High	Low	Min	Mean
Inactive	17.48	15.76	1.030	0.4125	1.396
Active	17.72	16.30	15.78	14.86	15.76

15.8.2 Inquiring and Paging State

	Current Consumption [mA]				
State	Max	High	Low	Min	Mean
Inquiring	218.4	213.5	65.13	44.54	114.3
Paging	215.1	213.9	64.62	43.65	112.8

15.8.3 Discoverable and Connectable State

Inquiry Scan [ms]		Page Scan [ms]		Current Consumption [mA]				
Interval	Window	Interval	Window	Max	High	Low	Min	Mean
2560	11.25	0	0	64.91	64.47	1.158	0.7186	1.892
160	160	0	0	66.10	65.44	16.49	14.10	64.64
0	0	2560	11.25	63.70	63.27	1.173	0.6170	1.854
0	0	160	160	65.94	65.18	45.72	45.00	64.84
2560	11.25	2560	11.25	65.45	65.01	1.274	0.7033	2.264
160	80	160	80	66.03	65.22	16.36	10.91	63.46
1280	11.25	640	50	66.34	65.63	1.444	0.8674	7.534

15.8.4 RFCOMM Connected State

The following results were measured when the role was master.

Sniff Parameters (ms)			Hold Parameters	Extra Details		Current Consumption [mA]				
Interval	Attempt	Timeout	Interval (ms)	Data	Audio	Max	High	Low	Min	Mean
-	-	-	-	No	No	208.1	205.9	1.304	0.6952	10.08
-	-	-	-	M Ÿ S	No	209.3	207.1	16.20	6.055	43.04
-	-	-	-	S Ÿ M	No	209.8	205.1	16.23	0.8984	40.20
-	-	-	-	No	HV1	207.9	205.5	65.56	42.02	89.04
-	-	-	-	No	HV2	210.1	205.3	41.65	13.80	63.32
-	-	-	-	No	HV3	210.9	209.0	16.70	0.8826	48.24
160	9.375	9.375	-	No	No	209.6	207.0	1.371	0.7582	4.881
160	9.375	9.375	-	No	HV1	207.8	205.4	65.12	42.28	88.99
160	9.375	9.375	-	No	HV2	209.2	204.8	41.55	14.27	61.02
160	9.375	9.375	-	No	HV3	209.6	208.2	15.95	0.6170	44.62
1000	9.375	9.375	-	No	No	205.7	204.7	1.329	0.7267	2.255
1000	9.375	9.375	-	No	HV1	206.4	204.0	64.30	43.41	88.20
1000	9.375	9.375	-	No	HV2	209.4	204.6	16.19	15.62	60.19
1000	9.375	9.375	-	No	HV3	209.9	207.6	16.13	0.7892	43.96
-	-	-	4000	No	No	18.35	16.44	1.341	0.7734	1.767

The following results were measured when the role was slave.

Sniff Parameters (ms)			Hold Parameters	Extra Details		Current Consumption [mA]				
Interval	Attempt	Timeout	Interval (ms)	Data	Audio	Max	High	Low	Min	Mean
-	-	-	-	No	No	208.6	206.4	44.54	38.72	51.11
-	-	-	-	M Ÿ S	No	208.5	204.9	46.06	34.31	68.46
-	-	-	-	S Ÿ M	No	189.5	186.6	44.38	34.20	68.49
-	-	-	-	No	HV1	209.7	204.2	64.15	40.86	88.14
-	-	-	-	No	HV2	210.2	204.6	45.05	39.20	70.99
-	-	-	-	No	HV3	210.3	204.4	45.02	38.81	64.12
160	9.375	9.375	-	No	No	207.5	206.5	1.505	0.8984	6.006
160	9.375	9.375	-	No	HV1	209.0	203.6	65.00	40.80	87.72
160	9.375	9.375	-	No	HV2	209.1	204.0	16.37	2.422	57.89
160	9.375	9.375	-	No	HV3	209.4	203.9	16.23	12.96	48.92
1000	9.375	9.375	-	No	No	209.8	208.0	1.009	0.8049	2.556
1000	9.375	9.375	-	No	HV1	208.8	203.5	64.33	42.34	87.80
1000	9.375	9.375	-	No	HV2	209.8	204.3	16.43	3.297	56.67
1000	9.375	9.375	-	No	HV3	209.8	204.3	16.24	14.13	47.49
-	-	-	4000	No	No	18.13	16.49	1.436	0.8435	1.813

15.9 Interoperability Testing

15.9.1 Interoperability Test Procedure

Devices are determined interoperable with the firmware if the following actions are successfully carried out.

Serial Port Profile (SPP)

1. Register the Serial Port Profile service.
2. Pair with the remote device to generate the link key.
3. Establish the connection to the remote device using this link key.
4. Communicate with the remote device.

Dialup Networking Profile (DUN)

1. Register the Dialup Networking Profile service.
2. Pair with the remote device to generate the link key.
3. Establish the connection to the remote device using this link key.
4. Monitor the encrypted data on the air.
5. Communicate with the remote device to browse the web.

Headset Profile (HSP)

1. Register the Headset Profile service.
2. Pair with the remote device to generate the link key.
3. Establish the connection to the remote device using this link key.
4. Hear the ring tone from the headset (HS) when the audio gateway (AG) rings the HS.
5. Confirm voice communication when the HS button is pressed.
6. Control the volume of the HS from the AG if the HS supports the remote audio control.
7. Press the volume button of the HS to indicate the volume of the HS to the AG if the HS supports the remote audio control.
8. Confirm audio disconnection when the HS button is pressed again.

Hands-Free Profile (HFP)

1. Register the Hands-Free Profile service.
2. Pair with the remote device to generate the link key.
3. Establish the connection to the remote device using this link key.
4. Hear the ring tone from the hands-free unit (HF) when the AG rings the HF.
5. Confirm voice communication when the HF button is pressed.
6. Control the volume of the HF from the AG if the HF supports the remote volume control in the supported features.
7. Press the volume button of the HF to indicate the volume to the AG if the HF supports the remote volume control in the supported features.
8. Confirm audio disconnection when the HF button is pressed again.

Object Push Profile (OPP)

1. Register the Object Push Profile service.
2. Pair with the remote device to generate the link key.
3. Establish the connection to the remote device using this link key.
4. Communicate with the remote device.

15.9.2 Test Results

The following table shows the results of this test.

Manufacturer	Product Name	Profiles				
		SPP	DUN (DT)	HSP (HS)	HFP (HF)	OPP
GN Netcom A/S	Bluetooth Headset BT200	---	---	OK	---	---
SIEMENS	Bluetooth Headset HHB-500	---	---	OK	---	---
Nokia	Bluetooth Headset HDW-2	---	---	OK	OK	---
Sony Ericsson	Bluetooth Headset HBH-60	---	---	OK	OK	---
Nokia	Bluetooth Car Kit CARK112	---	---	---	OK	---
Motorola	Bluetooth Car Kit HFW8000	---	---	OK	OK	---
Sony Ericsson	Bluetooth Car Kit HCB-30	---	---	OK	OK	---
IVT	BlueSoleil v1.2.0	OK	OK	---	---	OK
Compaq	iPAQ 3970	OK		---	---	OK
Ericsson	Mobile Telephone T39m	OK	---	---	---	OK
Sony Ericsson	Mobile Telephone T68i	OK	---	---	---	OK
Nokia	Mobile Telephone 3650	OK	---	---	---	OK
Sony	cdmaOne C413S PTX-600	---	---	---	---	OK