2.5 CONFORMANCE

If conformance to this profile is claimed, all capabilities indicated as mandatory for this profile shall be supported in the specified manner (process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth certification program.

3 APPLICATION LAYER

This section describes the feature requirements on units complying with the Headset profile.

Table 3.1 shows the feature requirements made by this profile.

	Feature	Support in HS	Support in AG
1.	Incoming audio connection	M	M
2.	Outgoing audio connection	M	O
3.	Audio connection transfer	M	M
4.	Remote audio volume control	O	O

Table 3.1: Application layer procedures

In the table above, incoming and outgoing shall be interpreted from the headset (HS) point of view.

Table 3.2 maps each feature to the procedures used for that feature. All procedures are mandatory if the feature is supported.

	Feature	Procedure	Ref.
1.	Incoming audio connection	Incoming audio connection establishment	4.2
		Audio connection release	4.4
2.	Outgoing audio connection	Outgoing audio connection establishment	4.3
		Audio connection release	4.4
3.	Audio connection transfer	Audio connection transfer	4.5
4.	Remote audio volume control	Remote audio volume control	4.6

Table 3.2: Application layer feature to procedure mapping

4 HEADSET CONTROL INTEROPERABILITY REQUIREMENTS

4.1 INTRODUCTION

The interoperability requirements for the Headset Control entity are completely contained in this chapter. Section 4.2 until 4.6 specify the requirements for the procedures directly relating to the application layer features.

Section 4.7 specifies the AT commands and results codes used for signalling purposes.

Section 4.8 specifies how the layers beneath the Headset Control entity are used to establish and release a connection.

4.2 INCOMING AUDIO CONNECTION

Upon an internal or user generated event, the AG will initiate connection establishment (see Section 4.8), and once the connection is established, will send an unsolicited result code RING to alert the user. The RING may be repeated for as long as the connection establishment is pending.

Optionally, the AG may provide an in-band ringing tone[1]. In this case, first SCO link establishment takes place.

[1] The in-band ringing tone is used to alert the user in the headset earpiece when the user is wearing the headset on his head.

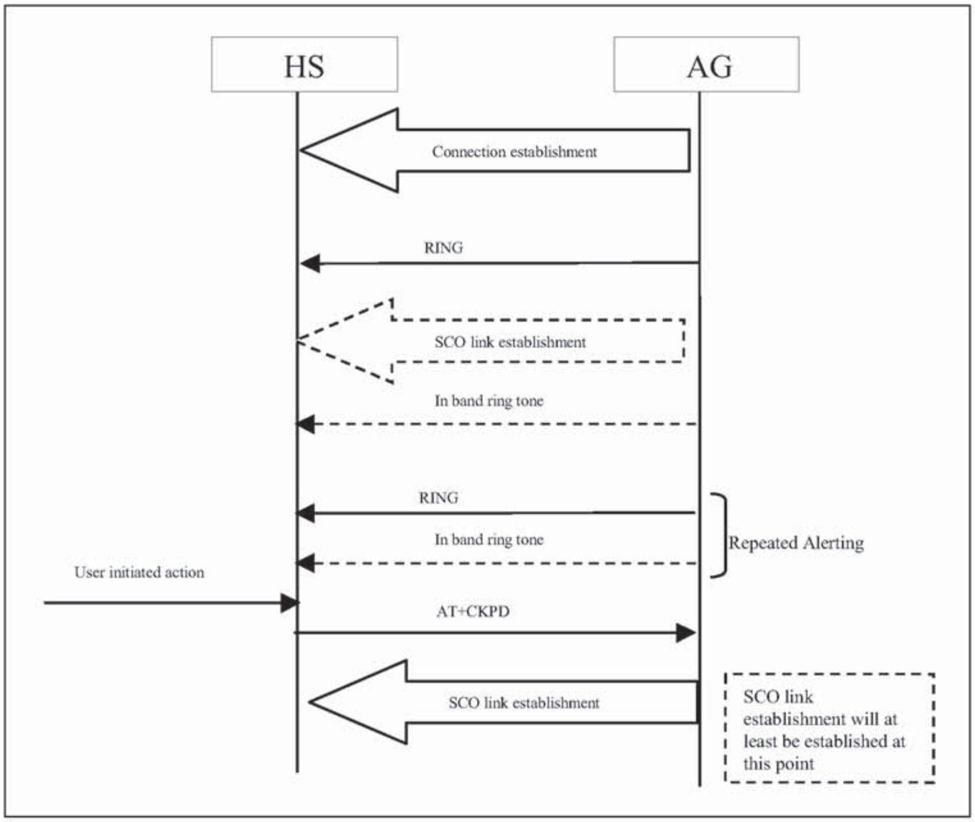

Figure 4.1: Incoming audio connection establishment

The user accepts the incoming audio connection by pressing the button on the headset. By doing this, the HS will send the AT+CKPD command (see Section 4.7) to the AG, whereupon the AG establishes the SCO link (if not already established).

4.3 OUTGOING AUDIO CONNECTION

An outgoing audio connection is initiated on the HS by pushing the button. The HS will initiate connection establishment (see Section 4.8), and will send the AT+CKPD command to the AG. Further internal actions may be needed on the AG to internally establish and/or route an audio stream to the HS[2].

The AG is responsible for establishing the SCO link.

[2] For a cellular phone a cellular call may need to be established, e.g. using last dialled number, pre-programmed number. For a personal computer this e.g. relates to playing a wav file, or audio CD.

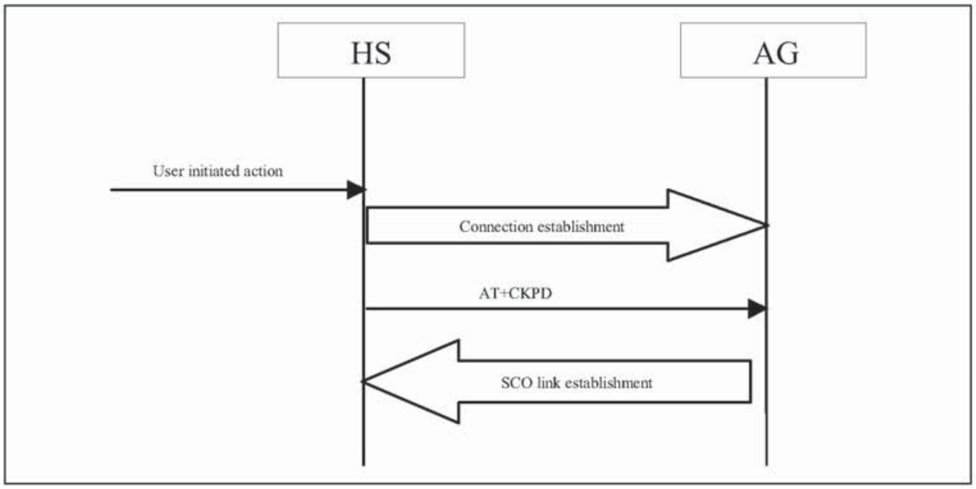

Figure 4.2: Outgoing audio connection establishment

4.4 AUDIO CONNECTION RELEASE

A call can be terminated either on the HS or on the AG. On the HS based upon the button being pushed, on the AG based upon internal actions or user intervention.

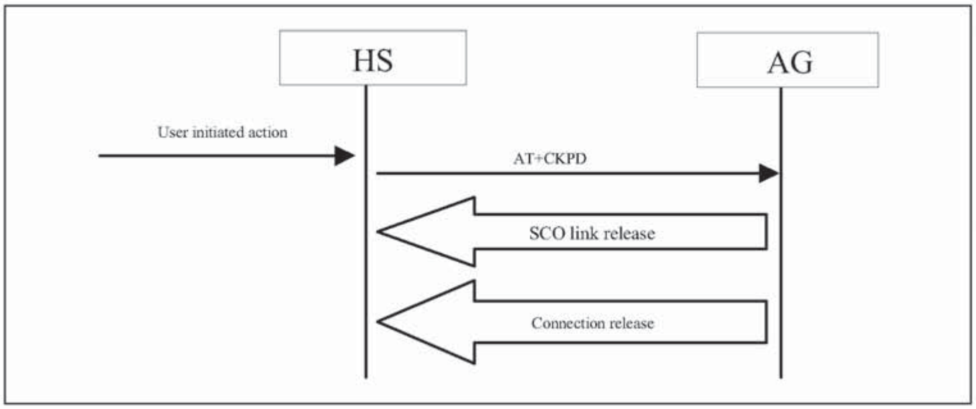

Figure 4.3: Audio connection release – HS initiated

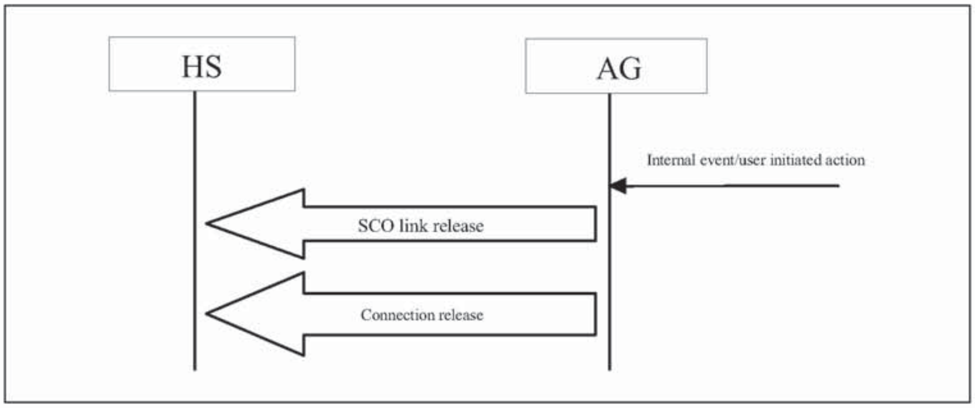

Figure 4.4: Audio connection release – AG initiated

Irrespective of the initiating side, the AG is responsible for releasing the connection (see Section 4.8).

4.5 AUDIO CONNECTION TRANSFER

An audio connection can be transferred from AG to HS or from HS to AG. The connection is transferred to the device initiating the transfer.

4.5.1 Audio connection transfer from AG to HS

The audio connection transfer from AG to HS is initiated by a user action on the HS side, which results in an AT+CKPD command being sent to the AG.

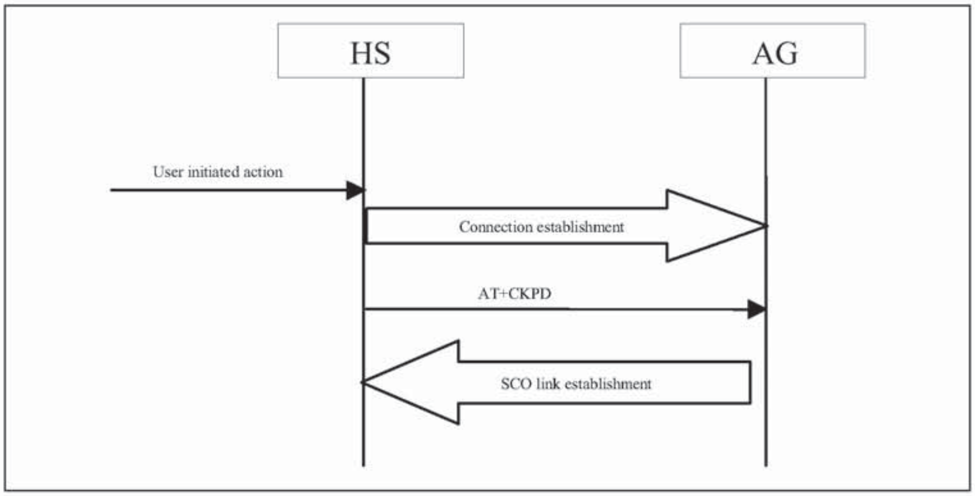

Figure 4.5: Audio connection transfer from AG to HS

4.5.2 Audio connection transfer from HS to AG

The audio connection transfer from HS to AG is initiated by a user action on the AG.

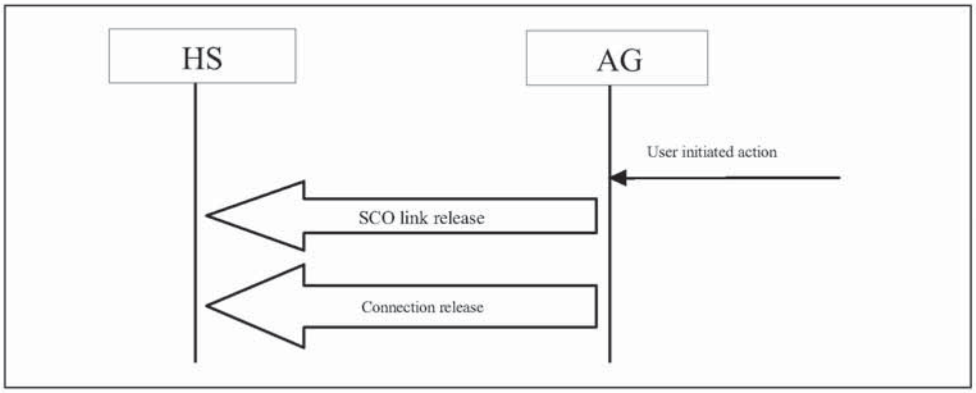

Figure 4.6: Audio connection transfer from HS to AG

4.6 REMOTE AUDIO VOLUME CONTROL

The AG can control the gain of the microphone and speaker of the HS by sending unsolicited result codes +VGM and +VGS respectively. There is no limit to the amount and order of result codes, as long as there is an active audio connection ongoing. When supporting the remote audio volume control, an implementation is not mandated to support both the control of the microphone volume and speaker volume.

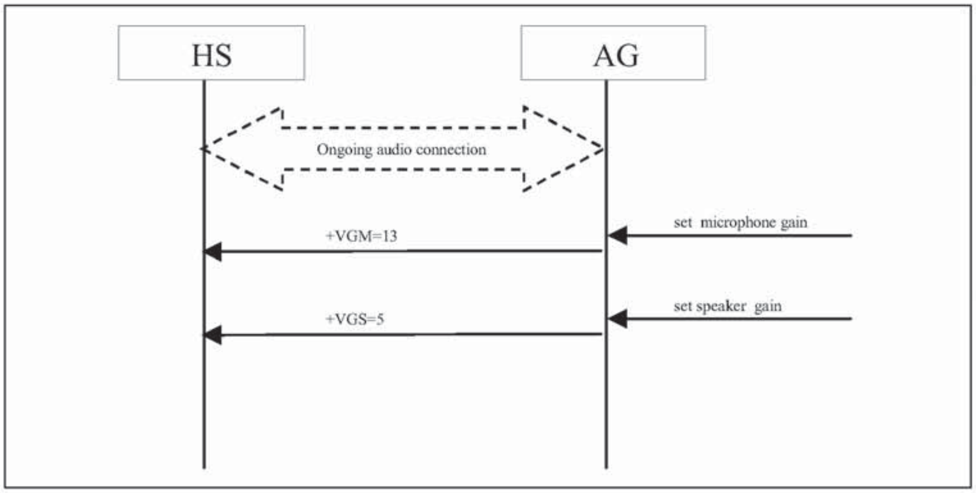

Figure 4.7: Audio volume control – example flow

Both the speaker and microphone gain are represented as parameter to the +VGS and +VGM, on a scale from 0 to 15. The values are absolute values, relating to a particular (implementation-dependent) volume level controlled by the HS.

The HS may store the VGS and VGM settings at connection release, to restore the volume levels at the next connection establishment. At connection establishment, the HS shall inform the AG of the (restored) volume levels using the AT commands +VGS and +VGM. In case local means are implemented on the HS to control the volume levels, the HS shall also use the AT commands +VGS and +VGM to inform the AG of any changes in the volume levels.

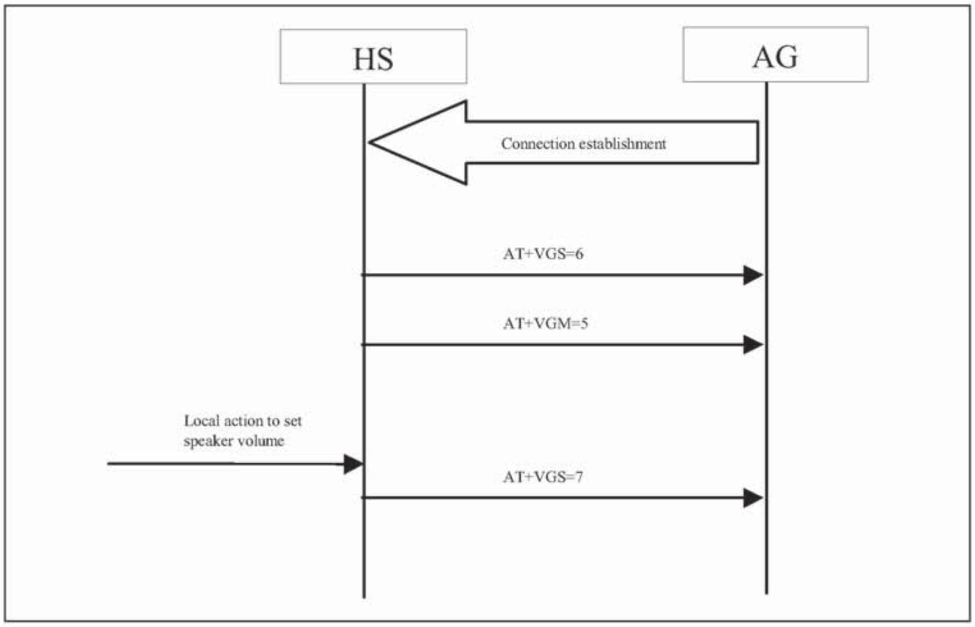

Figure 4.8: Volume level synchronization – example flow

4.7 AT COMMANDS AND RESULT CODES

4.7.1 General

For the exchange of the commands and unsolicited results codes, the format, syntax and procedures of V.250 [1] apply, with the exception that only one command (or unsolicited result code) per command line needs to be expected.

The headset profile uses a subset of AT commands and result codes from existing standards. These are listed in Section 4.7.2. For those AT commands and result codes where no existing commands applied, Section 4.7.3 defines additional ones.

4.7.2 AT capabilities re-used from V.250 and GSM 07.07

The mandatory set of AT commands and unsolicited result codes are indicated in Table 4.1 below.

AT capability	Description
RING	The Incoming call indication of V.250 [1], Section 6.3.4.
+CKPD	The keypad control command of GSM TS 07.07 [2], Section 8.7. For <keys>, the value of 200 indicates the Button on the headset being pushed. The <time> and <pause> parameters have no meaning in the headset profile.

Table 4.1: Mandatory AT capabilities

4.7.3 Bluetooth-defined AT capabilities

Optionally, the AT capabilities as indicated in Table 4.2 may be supported.

AT capability	Syntax	Description	Values
Microphone gain	+VGM=<gain >	Unsolicited result code issued by the AG to set the microphone gain of the HS. <gain> is an unsigned octet, relating to a particular (implementation-dependent) volume level controlled by the HS.	<gain>: 0-15
Speaker gain	+VGS=<gain>	Unsolicited result code issued by the AG to set the speaker gain of the HS. <gain> is an unsigned octet, relating to a particular (implementation-dependent) volume level controlled by the HS.	<gain>: 0-15

Table 4.2: Optional AT capabilities

AT capability	Syntax	Description	Values
Microphone gain level report	+VGM=<gain >	Command issued by the HS to report the current microphone gain level setting to the AG. <gain> is an unsigned octet, relating to a particular (implementation-dependent) volume level controlled by the HS.	<gain>: 0-15
Speaker gain level indication report	+VGS=<gain>	Command issued by the HS to report the current speaker gain level setting to the AG. <gain> is an unsigned octet, relating to a particular (implementation-dependent) volume level controlled by the HS.	<gain>: 0-15

Table 4.2: Optional AT capabilities

4.8 LOWER LAYER HANDLING

This section describes how the layers below the Headset Control entity are used to establish and release a connection.Section 4.8.1 describes how connections are handled when the PARK mode is not supported. Section 4.8.2 describes how connections are handled when the PARK mode is supported.

4.8.1 Connection handling without PARK mode

4.8.1.1 Connection establishment

Both the HS and the AG can initiate connection establishment. If there is no RFCOMM session between the AG and the HS, the initiating device shall first initialize RFCOMM. Connection establishment shall be performed as described in Section 7.3 of GAP and Section 3 of SPP.

4.8.1.2 Connection release

When the audio connection is released, the connection may be released as well. The AG always initiates connection release.

4.8.2 Connection handling with PARK mode

4.8.2.1 Connection establishment

If the PARK mode is supported, the connection is established once (e.g. on the first request for an audio connection). Later, when an audio connection is required, the parked device is unparked. In this section, for correct interpretation of the flows given in Section 4.2 to 4.6, the connection establishment is referred to as *initial* connection establishment, whereas the unparking is referred to as connection establishment.

Initial connection establishment shall be performed as described in Section 7.3 of GAP and Section 3 of SPP. Both sides may initiate the initial connection establishment. After initial connection establishment, the park mode is activated.

In Figure 4.9 the behavior is described in case an audio connection needs to be established – the parked device will be unparked. The unpark can be initiated from either side, depending where the request for an audio connection originated. If the PARK mode is used, neither RFCOMM DLCs nor the L2CAP channel is released.

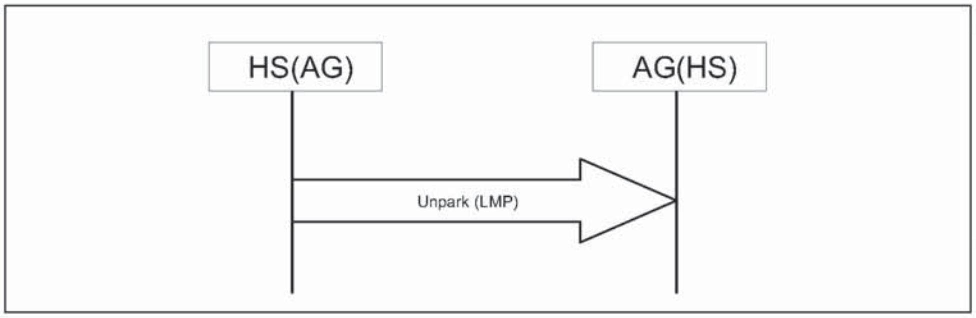

Figure 4.9: Connection establishment – Unparking a parked device

4.8.2.2 Connection release

When the audio connection is released, the connection is parked again, as indicated in Figure 4.10.

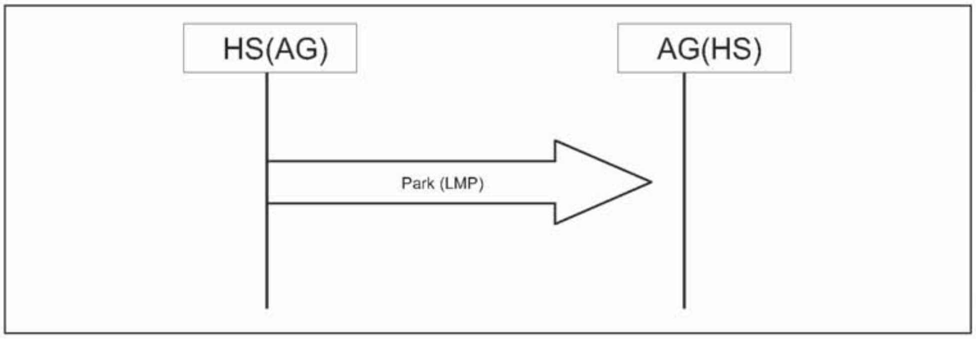

Figure 4.10: Connection release – Parking

When the audio connection is released, the complete connection may alternatively be released. The AG always initiates connection release.

5 SERIAL PORT PROFILE

This profile requires compliance with the Serial Port Profile. The following text together with the associated sub-clauses defines the requirements with regard to this profile, in addition to the requirements as defined in the Serial Port Profile.

As with the headset profile, both the AG and the HS can initiate connection establishment. For the purposes of reading the Serial Port Profile, both the AG and the HS can assume the role of Device A and B.

5.1 RFCOMM INTEROPERABILITY REQUIREMENTS

For the RFCOMM layer, no additions to the requirements as stated in the Serial Port Profile Section 4 shall apply.

5.2 L2CAP INTEROPERABILITY REQUIREMENTS

For the L2CAP layer, no additions to the requirements as stated in the Serial Port Profile Section 5 shall apply.

5.3 SDP INTEROPERABILITY REQUIREMENTS

This profile defines following service records for the headset and the audio gateway respectively.

The codes assigned to the mnemonics used in the Value column as well as the codes assigned to the attribute identifiers (if not specifically mentioned in the AttrID column) can be found in the Bluetooth Assigned Numbers section.

Item	Definition	Type	Value	AttrID	Status	Default
ServiceClassIDList					M	
ServiceClass0		UUID	Headset		M	
ServiceClass1		UUID	Generic Audio		M	
ProtocolDescriptorList					M	
Protocol0		UUID	L2CAP		M	
Protocol1		UUID	RFCOMM		M	
Protocol Specific Parameter0	Server Channel	Uint8	N=server channel #		M	
BluetoothProfile DescriptorList					O	
Profile0	Supported Profiles	UUID	Headset		M	Headset
Param0	Profile Version	Uint16	0x0100*		M	0x0100
ServiceName	Display-able Text name	String	Service-provider defined		O	'Headset'
Remote audio volume control		Bool-ean	True/False		O	False

Table 5.1: Service Record for Headset

*. Indicating version 1.0

Item	Definition	Type	Value	AttrID	Status	Default
ServiceClassIDList					M	
ServiceClass0		UUID	Headset		M	
ServiceClass1		UUID	Generic Audio		M	
ProtocolDescriptorList					M	
Protocol0		UUID	L2CAP		M	
Protocol1		UUID	RFCOMM		M	
Protocol Specific Parameter0	Server Channel	Uint8	N=server channel #		M	
BluetoothProfile DescriptorList						
Profile0	Supported Profile	UUID	Headset		M	Headset
Param0	Profile Version	Uint16	0x0100*		M	0x0100
ServiceName	Display-able Text name	String	Service-provider defined		O	'Voice gateway'

Table 5.2: Service Record for the Audio Gateway

*. Indicating version 1.0

5.4 LINK MANAGER (LM) INTEROPERABILITY REQUIREMENTS

In addition to the requirements for the Link Manager as stated in the "Serial Port Profile" on page 165, this profile mandates support for SCO links, in both the HS and AG.

5.5 LINK CONTROL (LC) INTEROPERABILITY REQUIREMENTS

In the table below, changes to the support status as listed in the Serial Port Profile, Section 8, Table 8.1 on page 184 are listed.

	Capability	Support in baseband	Support in AG	Support in HS
1.	Inquiry	M		X
2.	Inquiry scan	M	X	
3.	Paging	M		
4.	Page scan			
A	Type R0	M		
B	Type R1	M		
C	Type R2	M		
7.	Voice codec			
C	CVSD	O	M	M

Table 5.3: LC capabilities

5.5.1 Class of Device

A device which is active in the HS role shall, in the Class of Device field:

1. Set the bit 'Audio' in the Service Class field
2. Indicate 'Audio' as Major Device class
3. Indicate "Headset" as the Minor Device class

An inquiring AG may use this to filter the inquiry responses.

6 GENERIC ACCESS PROFILE

This section defines the support requirements for the capabilities as defined in Generic Access Profile.

6.1 MODES

The table shows the support status for Modes within this profile.

	Procedure	Support in HS	Support in AG
1	Discoverability modes		
	Non-discoverable mode	M	N/A
	Limited discoverable mode	O	N/A
	General discoverable mode	M	N/A
2	Connectability modes		
	Non-connectable mode	N/A	N/A
	Connectable mode	M	M
3	Pairing modes		
	Non-pairable mode	O	O
	Pairable mode	O	O

Table 6.1: Modes

6.2 SECURITY ASPECTS

No changes to the requirements as stated in the Generic Access Profile.

6.3 IDLE MODE PROCEDURES

The table shows the support status for Idle mode procedures within this profile.

	Procedure	Support in HS	Support in AG
1	General inquiry	N/A	M
2	Limited inquiry	N/A	O
3	Name discovery	N/A	O
4	Device discovery	N/A	O
5	Bonding	M (Note 1)	M (Note 1)
Note 1: Mandatory for the AG to support initiation of bonding, and for the HS to accept bonding.			

Table 6.2: Idle mode procedures

7 REFERENCES

[1] International Telecommunication Union, “ITU-T Recommendation V.250”

[2] ETS 300 916 (GSM 07.07) version 5.6.0

8 LIST OF FIGURES

9 LIST OF TABLES

Part K:7

DIAL-UP NETWORKING PROFILE

This profile defines the requirements for Bluetooth devices necessary for the support of the Dial-up Networking use case. The requirements are expressed in terms of end-user services, and by defining the features and procedures that are required for interoperability between Bluetooth devices in the Dial-up Networking use case.

CONTENTS

1 INTRODUCTION

1.1 SCOPE

The Dial-up Networking Profile defines the protocols and procedures that shall be used by devices implementing the usage model called 'Internet Bridge' (see Bluetooth SIG MRD). The most common examples of such devices are modems and cellular phones.

The scenarios covered by this profile are the following:

- Usage of a cellular phone or modem by a computer as a wireless modem for connecting to a dial-up internet access server, or using other dial-up services
- Usage of a cellular phone or modem by a computer to receive data calls

1.2 BLUETOOTH PROFILE STRUCTURE

In Figure 1.1, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure: a profile has dependencies on the profile(s) in which it is contained – directly and indirectly.

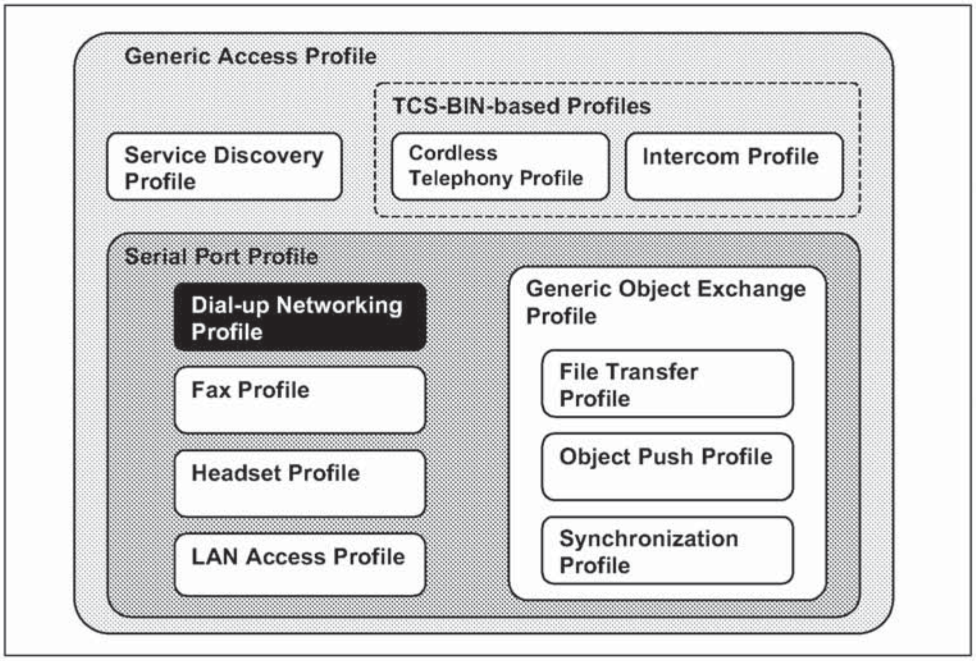

Figure 1.1: Bluetooth Profiles

1.3 SYMBOLS AND CONVENTIONS

1.3.1 Requirement status symbols

In this document, the following symbols are used:

'M' for mandatory to support (used for capabilities that shall be used in the profile);

'O' for optional to support (used for capabilities that can be used in the profile);

'C' for conditional support (used for capabilities that will be used in case a certain other capability is supported);

'X' for excluded (used for capabilities that may be supported by the unit but which shall never be used in the profile);

'N/A' for not applicable (in the given context it is impossible to use this capability).

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices following this profile. Therefore, these features shall never be activated while a unit is operating as a unit within this profile.

1.3.2 Signalling diagram conventions

The following arrows are used in diagrams describing procedures:

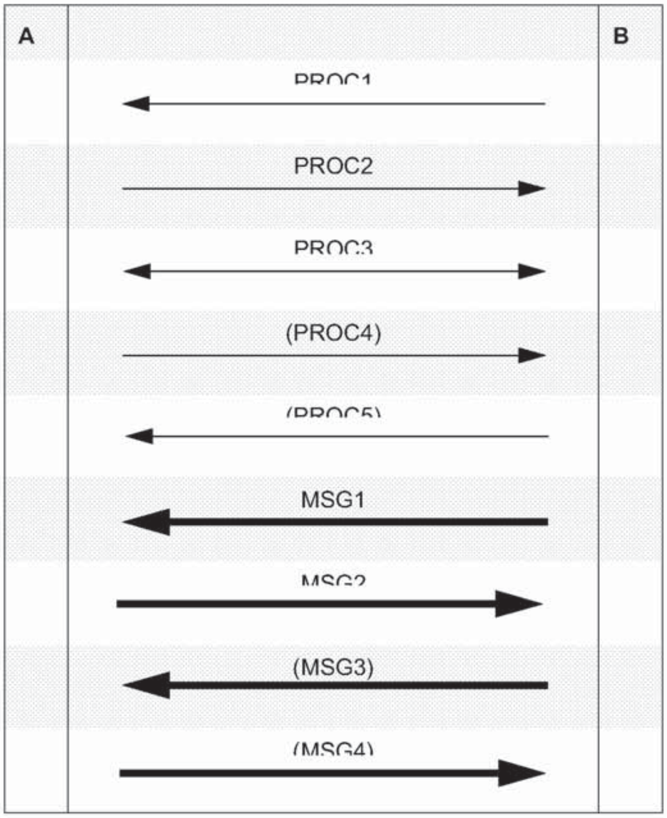

Table 1.1: Arrows used in signalling diagrams

In the table above, the following cases are shown: PROC1 is a sub-procedure initiated by B. PROC2 is a sub-procedure initiated by A. PROC3 is a sub-procedure where the initiating side is undefined (may be both A and B). PROC4 indicates an optional sub-procedure initiated by A, and PROC5 indicates an optional sub-procedure initiated by B.

MSG1 is a message sent from B to A. MSG2 is a message sent from A to B. MSG3 indicates an optional message from A to B, and MSG4 indicates an optional message from B to A.

1.3.3 Notation for timers and counters

Timers and counters may be introduced specific to this profile. To distinguish them from timers (counters) used in the Bluetooth protocol specifications and other profiles, these timers (counters) are named in the following format: ‘$\mathrm{T}_{\mathrm{DNF}}$*nnn*’ (‘$\mathrm{N}_{\mathrm{DNF}}$*nnn*’).

2 PROFILE OVERVIEW

2.1 PROFILE STACK

The figure below shows the protocols and entities used in this profile.

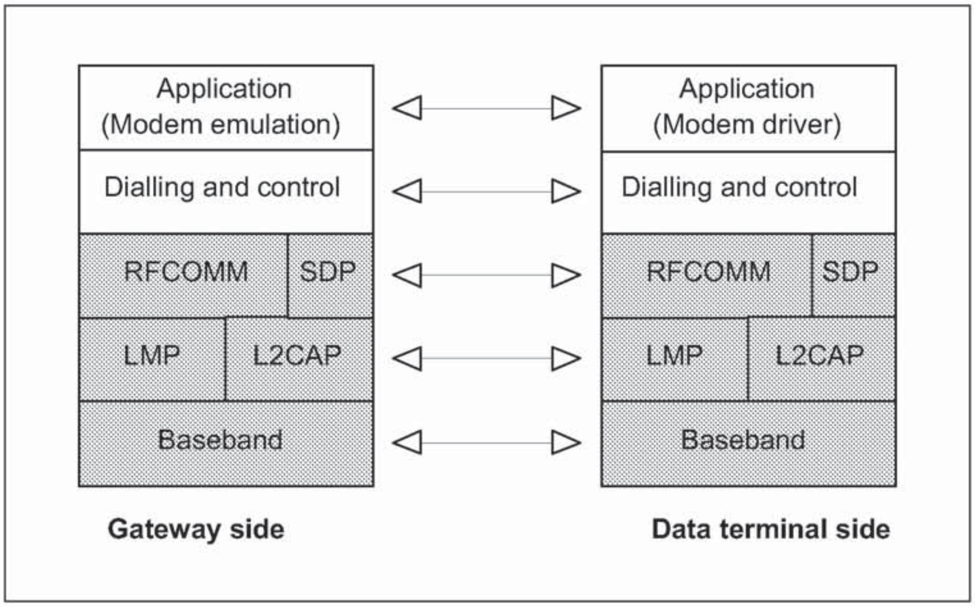

Figure 2.1: Protocol model

The Baseband, LMP and L2CAP are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM is the Bluetooth adaptation of GSM TS 07.10 [5], used for providing serial port emulation. SDP is the Bluetooth Service Discovery Protocol. Dialling and control (see Section 4) is the commands and procedures used for automatic dialling and control over the asynchronous serial link provided by the lower layers.

The modem emulation layer shown in Figure 2.1 is the entity emulating the modem, and the modem driver is the driver software in the data terminal.

For the shaded protocols/entities in Figure 2.1, The Serial Port Profile is used as base standard. For these protocols, all requirements stated in Serial Port Profile apply, except in those cases where this profile explicitly states deviations.

Note: Although not shown in the model above, it is assumed by this profile that the application layer has access to some lower layer procedures (for example SCO link establishment).

2.2 CONFIGURATIONS AND ROLES

The figures below show two typical configurations of devices for this profile:

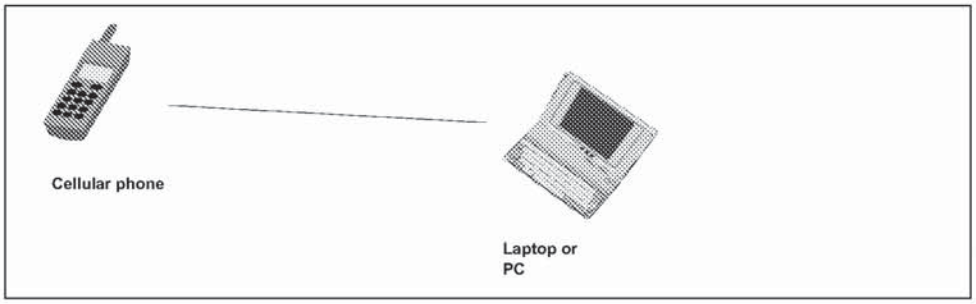

Figure 2.2: Dial-up Networking profile, example with cellular phone

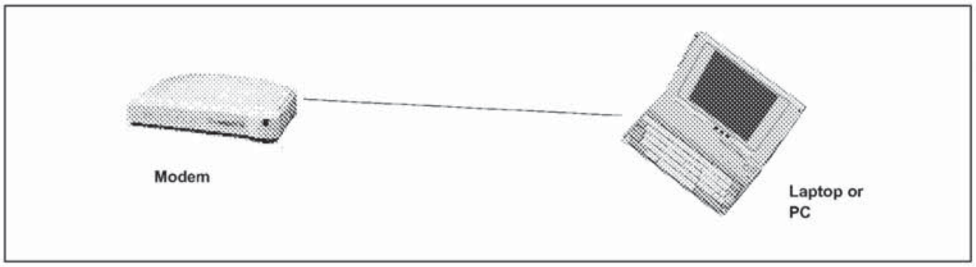

Figure 2.3: Dial-up Networking profile, example with modem

The following roles are defined for this profile:

Gateway (GW) – This is the device that provides access to the public network. Typical devices acting as gateways are cellular phones and modems.

Data Terminal (DT) – This is the device that uses the dial-up services of the gateway. Typical devices acting as data terminals are laptops and desktop PCs.

In the rest of this document, these terms are only used to designate these roles.

For purposes of mapping the Dial-up Networking profile to the conventional modem system architecture, the GW is considered Data Circuit Endpoint (DCE), and the DT is considered Data Terminal Endpoint (DTE).

2.3 USER REQUIREMENTS AND SCENARIOS

The scenarios covered by this profile are the following:

- Usage of a GW by a DT as a wireless modem for connecting to a dial-up internet access server or using other dial-up services
- Usage of a GW by a DT to receive data calls

The following restrictions apply to this profile:

a) The modem is not required to be able to report and/or discriminate between different call types for incoming calls.

b) This profile requires support for one-slot packets only. This means that this profile ensures that data rates up to 128 kbps can be used. Support for higher rates are optional.

c) Only one call at a time is supported.

d) The profile only supports point-to-point configurations.

e) There is no way defined in this profile to discriminate between two SCO channels originating from the same device. It is therefore manufacturer-specific as to how to deal with the situation where there are multiple applications requiring the use of multiple SCO channels originating from the same device.

f) Before a cellphone or modem can be used with a PC/Laptop for the first time, an initialization procedure must be performed. This typically involves manually activating initialization support, and entering a PIN code on the PC/Laptop keyboard (see Generic Access Profile for more details). This procedure may have to be repeated under certain circumstances.

g) This profile does not support multiple instances of its implementation in the same device.

Security is ensured by authenticating the other party upon connection establishment, and by encrypting all user data. The baseband and LMP mechanisms for authentication and encryption are used.

2.4 PROFILE FUNDAMENTALS

Before a DT can use the services of a GW for the first time, the two devices have to initialize. Initialization includes exchanging a PIN code, creation of link keys and service discovery.

A link has to be established before calls can be initiated or received. This requires paging of the other device. Link establishment is always initiated by the DT.

There are no fixed master/slave roles.

The GW and DT provide serial port emulation. For the serial port emulation, the serial port profile (see Serial Port Profile) is used. The serial port emulation is used to transport the user data, modem control signals and AT commands between the GW and the DT. AT-commands are parsed by the GW and responses are sent to the DT.

An SCO link is used to transport audio.

For security purposes, authentication is used, and all user data is encrypted. For this, the baseband/LMP mechanisms are used.

2.5 CONFORMANCE

If conformance to this profile is claimed, all capabilities indicated mandatory for this profile shall be supported in the specified manner (process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth certification program.

3 APPLICATION LAYER

This section describes the service requirements on units active in the Dial-up Networking profile.

3.1 SERVICE OVERVIEW

Table 3.1 shows the required services:

	Services	Support in DT	Support in GW
1.	Data call without audio feedback	M	M
2.	Data call with audio feedback	O	O
3.	Fax services without audio feedback	N/A	N/A
4.	Fax services with audio feedback	N/A	N/A
5.	Voice call	N/A	N/A

Table 3.1: Application layer procedures

3.2 DATA CALLS

The support of data calls is mandatory for both GWs and DTs. Optionally, audio feedback may be provided (see Section 4.2).

The GW shall emulate a modem connected via a serial port. The Serial Port Profile is used for RS-232 emulation, and a modem emulation entity running on top of the serial port profile provides the modem emulation.

3.3 FAX SERVICE

The support of fax is not covered by this profile. Refer to Fax Profile.

3.4 VOICE CALLS

The support of voice calls is not covered by this profile.

4 DIALLING AND CONTROL INTEROPERABILITY REQUIREMENTS

4.1 AT COMMAND SET USED

To guarantee that basic functionality can always be provided, it is required that a GW device supports the commands and responses as defined in the following sub-clauses.

The commands are based on ITU-T V.250 and GSM 07.07.

4.1.1 Command syntax

For the exchange of the commands, responses and unsolicited results codes, the format, syntax and procedures of ITU-T V.250 [6] apply.

4.1.2 Commands

The table below lists all commands that shall be supported by the GW.

Name	Description	Reference
&C	Circuit 109 (Received line signal detector) Behavior	Shall be supported as defined in [6].
&D	Circuit 108 (Data terminal ready) Behavior	Shall be supported as defined in [6].
&F	Set to Factory-defined Configuration	Shall be supported as defined in [6].
+GCAP	Request Complete Capabilities List	Shall be supported as defined in [6].
+GMI	Request Manufacturer Identification	Shall be supported as defined in [6].
+GMM	Request Model Identification	Shall be supported as defined in [6].
+GMR	Request Revision Identification	Shall be supported as defined in [6].
A	Answer	Shall be supported as defined in [6].
D	Dial	Shall be supported *either* as defined in [6] *or* as defined in [10].
E	Command Echo	Shall be supported as defined in [6].
H	Hook Control	Shall be supported as defined in [6].
L	Monitor Speaker Loudness	Shall be supported as defined in [6].
M	Monitor Speaker Mode	Shall be supported as defined in [6].

Table 4.1: Required commands

Name	Description	Reference
O	Return to Online Data State	Shall be supported as defined in [6].
P	Select Pulse Dialling	Shall be supported as defined in [6].
Q	Result Code Suppression	Shall be supported as defined in [6].
S0	Automatic Answer	Shall be supported as defined in [6].
S10	Automatic Disconnect Delay	Shall be supported as defined in [6].
S3	Command Line Termination Character	Shall be supported as defined in [6].
S4	Response Formatting Character	Shall be supported as defined in [6].
S5	Command Line Editing Character	Shall be supported as defined in [6].
S6	Pause Before Blind Dialling	Shall be supported as defined in [6].
S7	Connection Completion Timeout	The setting of this parameter may be ignored. If not ignored, it shall be supported as defined in [6].
S8	Comma Dial Modifier Time	Shall be supported as defined in [6].
T	Select Tone Dialling	Shall be supported as defined in [6].
V	DCE Response Format	Shall be supported as defined in [6].
X	Result Code Selection and Call Progress Monitoring Control	Shall be supported as defined in [6].
Z	Reset To Default Configuration	Shall be supported as defined in [6].

Table 4.1: Required commands

4.1.3 Result codes

The table below lists all result codes that shall be supported by the GW.

Name	Description	Reference
OK	Acknowledges execution of a command.	Shall be supported as defined in [6].
CONNECT	Connection has been established.	Shall be supported as defined in [6].
RING	The DCE has detected an incoming call signal from the network.	Shall be supported as defined in [6].
NO CARRIER	The connection has been terminated, or the attempt to establish a connection failed.	Shall be supported as defined in [6].
ERROR	Error.	Shall be supported as defined in [6].
NO DIALTONE	No dial-tone detected.	Shall be supported as defined in [6].
BUSY	Busy signal detected.	Shall be supported as defined in[6].

Table 4.2: Required result codes

4.2 CALL PROGRESS AUDIO FEEDBACK

The GW or DT may optionally be able to provide audio feedback during call establishment. This clause applies only to gateways/data terminals that are able to provide audio feedback.

SCO links are used to transport the digitized audio over the Bluetooth link. The GW shall take all initiatives for SCO link establishment. The setting of the M parameter (see [6], Section 6.3.14) controls whether audio feedback is provided by the GW.

If a GW provides audio feedback for a call, the GW shall use the initiate SCO link procedure (see Link Manager protocol) to establish the audio link when the DCE goes off-hook.

Depending on the setting of the M parameter, the GW releases the audio link when the DCE has detected a carrier or when the DCE goes on-hook. The remove SCO link procedure (see [Link Manager protocol]) shall be used for audio link release.

If SCO link establishment fails, the call establishment shall proceed without the audio feedback.

This profile assumes that the DT is not active in any other profile which uses SCO links while it is operating in the Dial-up Networking profile. Therefore, the behavior in a situation where multiple SCO links are established simultaneously is undefined.

4.3 ESCAPE SEQUENCE

It is recommended that the GW supports an escape sequence (i.e. a sequence of characters which causes the GW to leave the online data state and go to the online command state). This profile does not mandate a particular escape sequence – it is up to the implementer of the profile if and how returning to command mode is supported.

5 SERIAL PORT PROFILE INTEROPERABILITY REQUIREMENTS

This profile requires compliance to the Serial Port Profile. For the purposes of reading the Serial Port Profile, the GW shall always be considered to be Device B and the DT shall always be considered to be Device A.

The following text together with the associated sub-clauses define the requirements with regards to this profile, in addition to the requirements defined in Serial Port Profile.

5.1 RFCOMM INTEROPERABILITY REQUIREMENTS

For RFCOMM, no additions to the requirements stated in Serial Port Profile apply.

5.2 L2CAP INTEROPERABILITY REQUIREMENTS

For the L2CAP layer, no additions to the requirements stated in Serial Port Profile apply.

5.3 SDP INTEROPERABILITY REQUIREMENTS

Table 5.1 lists all entries in the SDP database of the GW defined by this profile. The 'Status' column indicates whether the presence of this field is mandatory or optional.

The codes assigned to the mnemonics used in the 'Value' column, and the codes assigned to the attribute identifiers, can be found in the Bluetooth Assigned Numbers section.

Item	Definition:	Type:	Value:	Status	Default
Service Class ID List				M	
Service Class #0		UUID	Generic Networking	O	
Service Class #1		UUID	Dial-up Networking	M	
Protocol Descriptor List				M	
Protocol #0		UUID	L2CAP	M	
Protocol #1		UUID	RFCOMM	M	

Table 5.1: Service Database Entries

Item	Definition:	Type:	Value:	Status	Default
Parameter for Protocol #1	Server Channel	UInt8	1,2,3,...,30	M	
Service Name	Displayable Text name	String	Service-provider defined	O	'Dial-up networking'
Audio Feedback Support		Boolean	True/False	O	False
BluetoothProfile-DescriptorList				M	
Profile #0		UUID	Dial-up Networking	M	
Parameter for Profile #0	Version	UInt16	0x0100*	O	0x100

Table 5.1: Service Database Entries

*. Indicating version 1.0

5.4 LINK MANAGER (LM) INTEROPERABILITY REQUIREMENTS

In addition to the requirements for the Link Manager as stated in the "Serial Port Profile" on page 165, this profile requires support for SCO links, in both the GW and DT. The support is conditional upon the ability to provide audio feedback."

5.5 LINK CONTROL (LC) INTEROPERABILITY REQUIREMENTS

In the table below, all LC capabilities required by this profile are listed.

	Capabilities	Support in baseband	Support in GW	Support in DT
5.	Packet types			
N	HV3 packet	O	C1	C2
7.	Voice codec			
C	CVSD	O	C1	C2
C1: The support for this capability is mandatory for gateways that are able to provide audio feedback to the DT. C2: The support for this capability is mandatory for data terminals that are able to provide audio feedback to the user.				

Table 5.2: Baseband/LC capabilities

5.5.1 Class of Device usage

A device which is active in the GW role of the Dial-up Networking profile shall, in the Class of Device field:

1. Set the bits ‘Telephony’ and ‘Networking’ in the Service Class field (see Bluetooth Assigned Numbers)
2. Indicate ‘Phone’ as Major Device class (see Bluetooth Assigned Numbers)

This may be used by an inquiring device to filter the inquiry responses.

6 GENERIC ACCESS PROFILE INTEROPERABILITY REQUIREMENTS

This profile requires compliance to the Generic Access Profile.

This section defines the support requirements with regards to procedures and capabilities defined in Generic Access Profile.

6.1 MODES

The table shows the support status for Modes within this profile.

	Procedure	**Support in DT**	**Support in GW**
1	Discoverability modes		
	Non-discoverable mode	N/A	M
	Limited discoverable mode	N/A	O
	General discoverable mode	N/A	M
2	Connectability modes		
	Non-connectable mode	N/A	X
	Connectable mode	N/A	M
3	Pairing modes		
	Non-pairable mode	M	M
	Pairable mode	O	M

Table 6.1: Modes

6.2 SECURITY ASPECTS

The table shows the support status for Security aspects within this profile

	Procedure	**Support in DT**	**Support in GW**
1	Authentication	M	M
2	Security modes		
	Security mode 1	N/A	X
	Security mode 2	C1	C1
	Security mode 3	C1	C1
C1: Support for at least one of the security modes 2 and 3 is mandatory.			

Table 6.2: Security aspects

6.3 IDLE MODE PROCEDURES

The table shows the support status for Idle mode procedures within this profile

	Procedure	Support in DT	Support in GW
1	General inquiry	M	N/A
2	Limited inquiry	O	N/A
3	Name discovery	O	N/A
4	Device discovery	O	N/A
5	Bonding	M (Note 1)	M (Note 1)
Note 1: See section 6.3.1			

Table 6.3: Idle mode procedures

6.3.1 Bonding

It is mandatory for the DT to support initiation of bonding, and for the GW to accept bonding.

7 REFERENCES

[1] Bluetooth Baseband specificationt

[2] Bluetooth Link Manager Protocol

[3] Bluetooth Logical Link Control and Adaptation Protocol Specification

[4] RFCOMM with TS 07.10

[5] TS 101 369 (GSM 07.10) version 6.1.0

[6] International Telecommunication Union, “ITU-T Recommendation V.250”

[7] Bluetooth Service Discovery Protocol

[8] John Webb, “Bluetooth SIG MRD”, version 1.0 Draft

[9] Bluetooth Serial Port Profile

[10] ETS 300 916 (GSM 07.07) version 5.6.0

[11] Bluetooth Fax Profile

[12] Bluetooth Assigned Numbers

8 LIST OF FIGURES

9 LIST OF TABLES

Part K:8

FAX PROFILE

This profile defines the requirements for Bluetooth devices necessary for the support of the Fax use case. The requirements are expressed in terms of end-user services, and by defining the features and procedures that are required for interoperability between Bluetooth devices in the Fax use case.

CONTENTS

1 INTRODUCTION

1.1 SCOPE

The Fax profile defines the protocols and procedures that shall be used by devices implementing the fax part of the usage model called 'Data Access Points, Wide Area Networks' (see Bluetooth SIG MRD).

A Bluetooth cellular phone or modem may be by a computer as a wireless fax modem to send or receive a fax message.

1.2 PROFILE DEPENDENCIES

In Figure 1.1, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure: a profile has dependencies on the profile(s) in which it is contained – directly and indirectly.

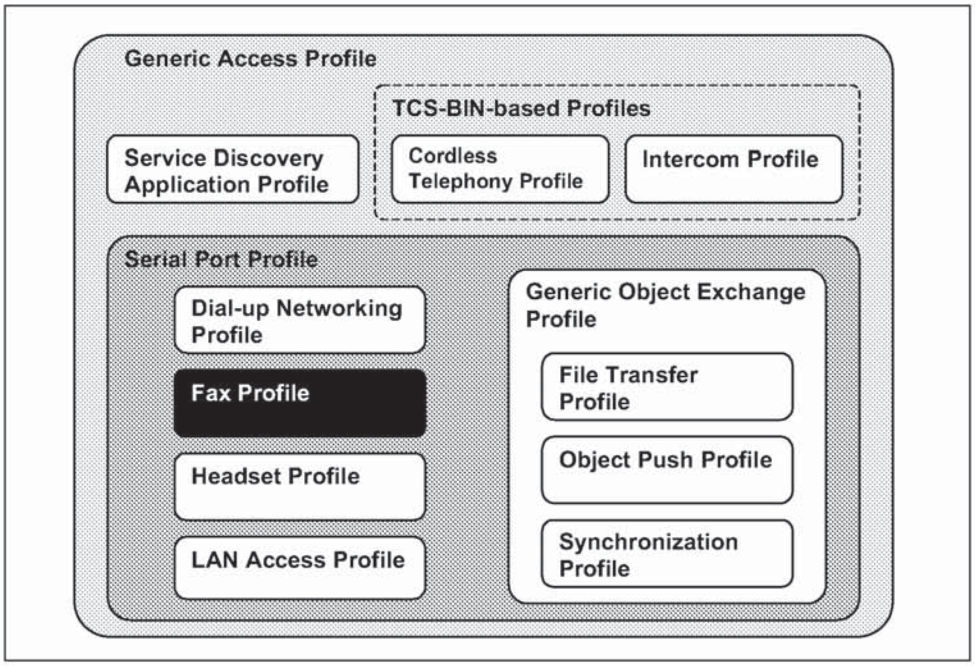

Figure 1.1: Bluetooth Profiles

As indicated in the figure, the Fax profile is dependent upon both the Serial Port Profile and the Generic access profile – details are provided in Section 5 Serial Port Profile on page 256 and Section 6 Generic Access Profile Interoperability Requirements on page 259.

1.3 SYMBOLS AND CONVENTIONS

1.3.1 Requirement status symbols

In this document, the following symbols are used:

- 'M' for mandatory to support
- 'O' for optional to support
- 'X' for excluded (used for capabilities that may be supported by the unit but which shall never be used in the use case)
- 'C' for conditional to support
- 'N/A' for not applicable (in the given context it is impossible to use this capability)

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices in this use case. Therefore, these features shall never be activated while a unit is operating as a unit within this use case.

Within the scope of this Fax profile, the expression 'Fax class" is used as a shortcut to 'facsimile service class" as defined by [2], [3], [4] and [4]. This is not to be confused with Bluetooth service class.

1.3.2 Signalling diagram conventions

The following arrows are used in diagrams describing procedures:

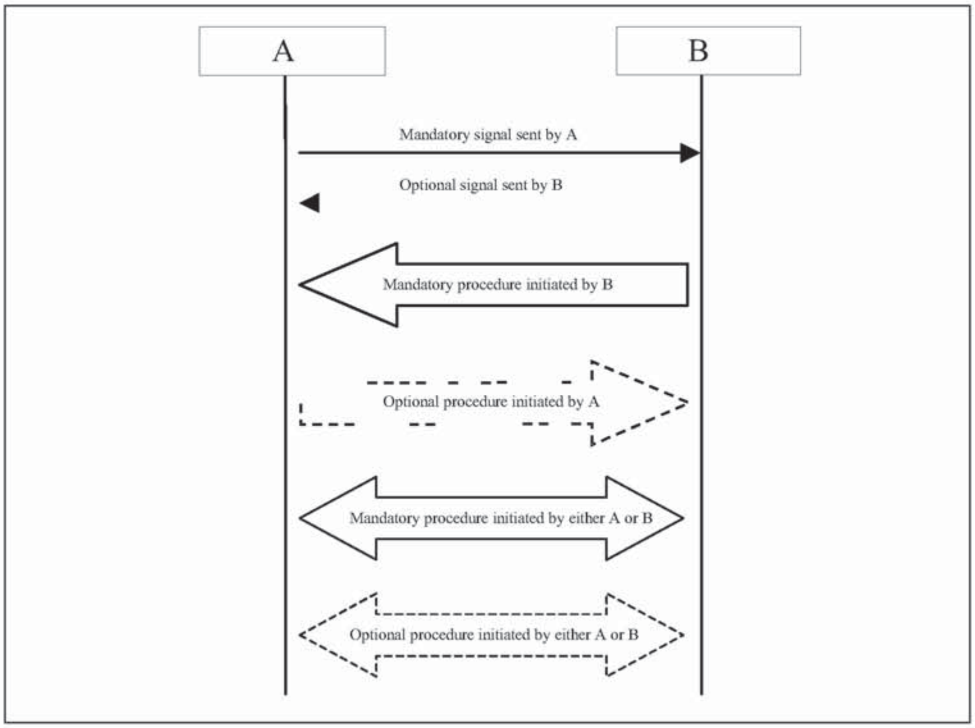
A
B
Mandatory signal sent by A
Optional signal sent by B
Mandatory procedure initiated by B
Optional procedure initiated by A
Mandatory procedure initiated by either A or B
Optional procedure initiated by either A or B

Figure 1-2 Arrows used in signalling diagrams

2 PROFILE OVERVIEW

2.1 PROFILE STACK

The figure below shows the protocols and entities used in this profile.

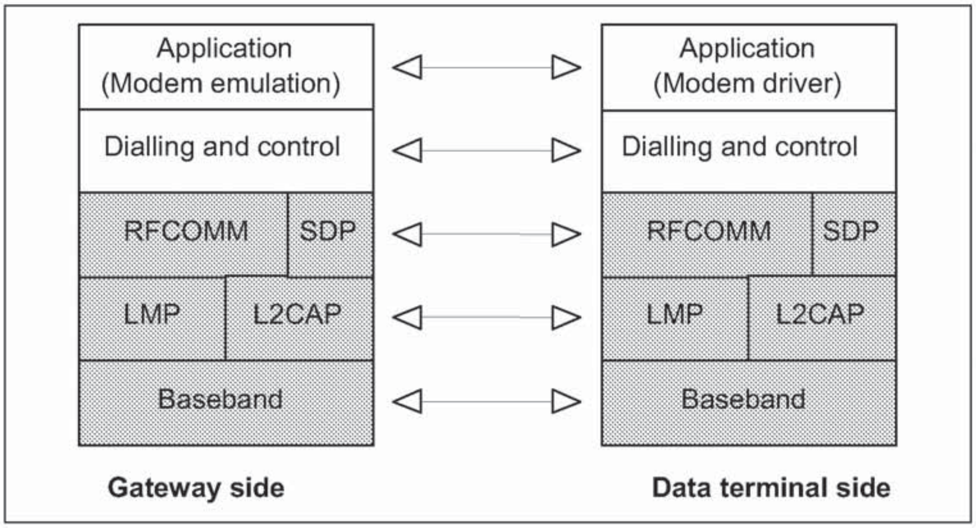

Figure 2.1: Protocol model

The Baseband, LMP and L2CAP are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM is the Bluetooth adaptation of GSM TS 07.10 [1], used for providing serial port emulation. SDP is the Bluetooth Service Discovery Protocol. Dialling and control (see Section 4) defines the commands and procedures used for automatic dialling and control over the asynchronous serial link provided by the lower layers.

The modem emulation layer shown in Figure 2.1 is the entity emulating the modem, and the modem driver is the driver software in the data terminal.

For the shaded protocols/entities in Figure 2.1, The Serial Port Profile is used as base standard. For these protocols, all requirements stated in Serial Port Profile apply, except in those cases where this profile explicitly states deviations.

Note: Although not shown in the model above, it is assumed by this profile that the application layer has access to some lower layer procedures (for example SCO link establishment).

2.2 CONFIGURATIONS AND ROLES

The figures below show two typical configurations of devices for this profile:

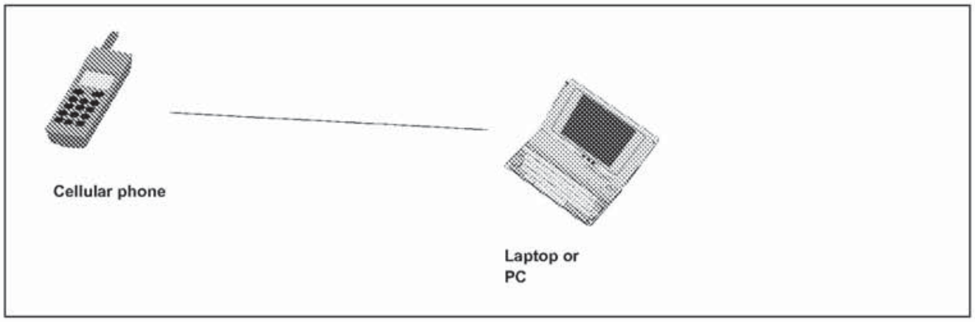

Figure 2.2: Fax profile, example with cellular phone

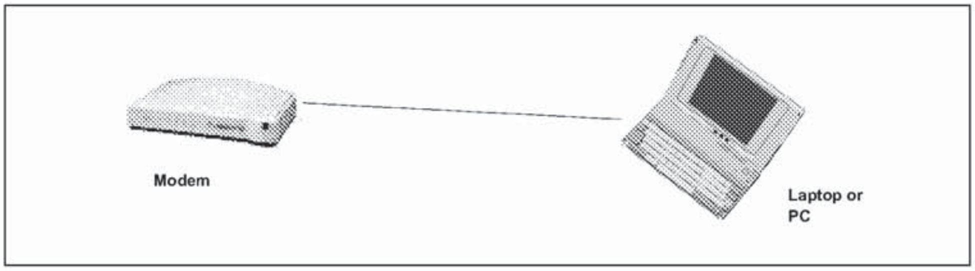

Figure 2.3: Fax profile, example with modem

The following roles are defined for this profile:

Gateway (GW) – This is the device that provides facsimile services. Typical devices acting as gateway are cellular phones and modems.

Data Terminal (DT) – This is the device that uses the facsimile services of the gateway. Typical devices acting as data terminals are laptops and desktop PCs.

In the rest of this document, these terms are only used to designate these roles.

For purposes of mapping the Fax profile to the conventional modem system architecture, the GW is considered Data Circuit Endpoint (DCE), and the DT is considered Data Terminal Endpoint (DTE).

2.3 USER REQUIREMENTS AND SCENARIOS

The Fax profile defines the usage of a GW by a DT as a wireless modem to send or receive fax messages

The following restrictions apply to this profile:

a) The GW (cellphone or modem) is not required to be able to report and/or discriminate between different call types for incoming calls.

b) This profile requires support for one-slot packets only. This means that this profile ensures that data rates up to 128 kbps can be used. Support for higher rates are optional.

c) Only one call at a time is supported.

d) The profile only supports point-to-point configurations.

e) Since in this profile there is no way defined to discriminate between 2 SCO channels originating from the same device, it is manufacturer specific as to deal with the situation where there are multiple applications requiring the use of multiple SCO channels originating from the same device.

f) This profile does not support multiple instances of its implementation in the same device.

2.4 PROFILE FUNDAMENTALS

Here is a brief summary of the interactions that take place when a DT wants to use the facsimile services of a GW.

1. If the DT does not have the Bluetooth Address of the GW, the DT has to obtain the address; e.g. using the Device discovery procedure, see Section 6.4 of Generic Access profile.
2. The Fax profile mandates the use of a secure connection through the authentication procedure (see Section 5.1 of Generic Access profile), and encryption of all user data through the baseband / LMP encryption mechanisms (see Section 8 of the Generic Access profile).
3. Link establishment is always initiated by the DT.
4. There are no fixed master / slave roles.
5. The fax call is established.
6. The GW and DT provide serial port emulation. For the serial port emulation, the serial port profile (see Serial Port Profile) is used. The serial port emulation is used to transport the user data, modem control signals and AT commands between the GW and the DT. AT-commands are parsed by the GW and responses are sent to the DT.
7. An optional SCO link may be used to transport fax audio feedback.
8. After the fax call has been cleared, the channel and link will be released as well.

2.5 CONFORMANCE

When conformance to this profile is claimed, all capabilities indicated mandatory for this profile shall be supported in the specified manner (process mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities, for which support is indicated, are subject to verification as part of the Bluetooth certification program.

3 APPLICATION LAYER

This section describes the service requirements on units active in the Fax profile.

3.1 SERVICE OVERVIEW

Table 3.1 shows the required services:

	Services	Support in DT	Support in GW
1.	Data call without audio feedback	N/A	N/A
2.	Data call with audio feedback	N/A	N/A
3.	Fax services without audio feedback	M	M
4.	Fax services with audio feedback	O	O
5.	Voice call	N/A	N/A

Table 3.1: Application layer procedures

3.2 DATA CALLS

The support of data calls is not covered by this profile.
Refer to Dial-up Networking Profile.

3.3 FAX SERVICE

At least one of the following fax classes of service is mandatory for both the GW and the paired DT (see Section 4.1.2):

Fax Class 1 TIA-578-A [2] and ITU T.31 [4]

Fax Class 2.0 TIA-592 [3]and ITU T.32 [5]

Fax Service Class 2 – No industry standard exists (manufacturer specific).

Optionally, audio feedback may be provided (see Section 4.2).

The GW shall emulate a modem connected via a serial port. The Serial Port Profile is used for RS-232 emulation, and RFCOMM running on top of the serial port profile provides the modem emulation.

3.4 VOICE CALLS

The support of voice calls is not covered by this profile. Refer to Cordless Telephony Profile.

4 DIALLING AND CONTROL INTEROPERABILITY REQUIREMENTS

4.1 AT COMMAND SET USED

To guarantee that basic functionality can always be provided, it is required that a GW device supports the commands and responses as defined in the supported fax class of service(s):

Fax Class 1 TIA-578-A [2] and ITU T.31 [4]

Fax Class 2.0 TIA-592 [3]] and ITU T.32 [5]

Fax Service Class 2 – No industry standard exists (manufacturer specific).

4.1.1 Command syntax, Protocols and Result Codes

Refer to each specific implemented fax service class document for a description of the required commands, protocols and result codes.

4.1.2 Fax Service Class selection procedure

This profile does not require a specific service class of fax. This profile supports 2 standards-based fax 'classes' – fax class 1 [2], [4] and fax class 2.0 [3], [5] – and a third manufacturer-specific pseudo-standard, fax class 2 (no industry reference standard exists).

The DT shall check the GW SDP or perform an 'AT+FCLASS" command to discover the fax class of service(s) supported by the GW.

Bluetooth devices implementing this profile must support a minimum of one fax service class, but may support any or all fax services classes.

4.2 CALL PROGRESS AUDIO FEEDBACK

The GW or DT may optionally be able to provide audio feedback during call establishment. This clause applies only to gateways/data terminals that are able to provide audio feedback.

SCO links are used to transport the digitized audio over the Bluetooth link. The GW shall take all initiatives for SCO link establishment. The setting of the M parameter (see [6], Section 6.3.14) controls whether the GW provides audio feedback.

If a GW provides audio feedback for a call, the GW shall use the 'initiate SCO link' procedure (see Link Manager protocol) to establish the audio link when the DCE goes off-hook.

Depending on the setting of the M parameter, the GW releases the audio link when the DCE has detected a carrier or when the DCE goes on-hook. The 'remove SCO link' procedure (see [Link Manager protocol]) shall be used for audio link release.

If SCO link establishment fails, the call establishment shall proceed without the audio feedback.

This profile assumes that the DT is not active in any other profile that uses SCO links while it is operating in the Fax profile. Therefore, behavior is not defined for a situation where multiple SCO links are established simultaneously.

5 SERIAL PORT PROFILE

This profile requires compliance to the Serial Port Profile. For the purposes of reading the Serial Port Profile, the GW shall always be considered to be Device B and the DT shall always be considered to be Device A.

The following text together with the associated sub-clauses define the requirements with regards to this profile in addition to the requirements defined in the Serial Port Profile.

5.1 RFCOMM INTEROPERABILITY REQUIREMENTS

For RFCOMM, no additions to the requirements stated in Serial Port Profile apply.

5.2 L2CAP INTEROPERABILITY REQUIREMENTS

For the L2CAP layer, no additions to the requirements stated in Serial Port Profile apply.

5.3 SDP INTEROPERABILITY REQUIREMENTS

Table 5.1 lists all entries in the SDP database of the GW defined by this profile. The 'Status' column indicates whether the presence of this field is mandatory or optional.

The codes assigned to the mnemonics used in the 'Value' column and the codes assigned to the attribute identifiers can be found in Bluetooth Assigned Numbers.

Item	Definition:	Type:	Value:	Status	Default
Service Class ID List				M	
Service Class #0		UUID	Generic Telephony	O	
Service Class #1		UUID	Fax	M	
Protocol Descriptor List				M	
Protocol #0		UUID	L2CAP	M	
Protocol #1		UUID	RFCOMM	M	
Parameter for Protocol #1	Server Channel	UInt8	N = server channel #	M	

Table 5.1: Service Database Entries

Item	Definition:	Type:	Value:	Status	Default
Service Name	Displayable Text name	String	Service-provider defined	O	'Fax'
Audio Feedback Support		Boolean	True/False	O	False
Fax Class 1 Support		Boolean	True/False	O	False
Fax Class 2.0 Support		Boolean	True/False	O	False
Fax Class 2 Support		Boolean	True/False	O	False
BluetoothProfile DescriptorList				M	
Profile #0		UUID	Fax	M	
Parameter for Profile #0	Version	UInt16	0x0100*	O	0x100

Table 5.1: Service Database Entries

*. Indicating version 1.0

5.4 LINK MANAGER (LM) INTEROPERABILITY REQUIREMENTS

In addition to the requirements for the Link Manager as stated in the "Serial Port Profile" on page 165, this profile requires support for SCO links, in both the GW and DT. The support is conditional upon the ability to provide audio feedback."

5.5 LINK CONTROL (LC) INTEROPERABILITY REQUIREMENTS

In the table below, all LC capabilities required by this profile are listed.

	Capabilities	Support in baseband	Support in GW	Support in DT
5.	Packet types			
N	HV3 packet	O	C1	C2
7.	Voice codec			
C	CVSD	O	C1	C2
C1: The support for this capability is mandatory for gateways that are able to provide audio feedback to the DT. C2: The support for this capability is mandatory for data terminals that are able to provide audio feedback to the user.				

Table 5.2: Baseband/LC capabilities

5.5.1 Class of Device usage

A device which is active in the GW role of the Fax profile shall, in the Class of Device field:

1. Set the 'Telephony' bit in the Service Class field (see Bluetooth Assigned Numbers)
2. Indicate 'Phone' as Major Device class (see Bluetooth Assigned Numbers)

This may be used by an inquiring device to filter the inquiry responses.

6 GENERIC ACCESS PROFILE INTEROPERABILITY REQUIREMENTS

This profile requires compliance to the Generic Access Profile.

This section defines the support requirements with regards to procedures and capabilities defined in Generic Access Profile.

6.1 MODES

The table shows the support status for Modes within this profile.

	Procedure	Support in DT	Support in GW
1	Discoverability modes		
	Non-discoverable mode	N/A	M
	Limited discoverable mode	N/A	O
	General discoverable mode	N/A	M
2	Connectability modes		
	Non-connectable mode	N/A	X
	Connectable mode	N/A	M
3	Pairing modes		
	Non-pairable mode	M	M
	Pairable mode	O	M

Table 6.1: Modes

6.2 SECURITY ASPECTS

The table shows the support status for Security aspects within this profile.

	Procedure	Support in DT	Support in GW
1	Authentication	M	M
2	Security modes		
	Security mode 1	N/A	X
	Security mode 2	C1	C1
	Security mode 3	C1	C1
C1: Support for at least one of the security modes 2 and 3 is mandatory			

Table 6.2: Security aspects

6.3 IDLE MODE PROCEDURES

The table shows the support status for Idle mode procedures within this profile.

	Procedure	Support in DT	Support in GW
1	General inquiry	M	N/A
2	Limited inquiry	O	N/A
3	Name discovery	O	N/A
4	Device discovery	O	N/A
5	Bonding	M (Note 1)	M (Note 1)
Note 1: See section 6.3.1			

Table 6.3: Idle mode procedures

6.3.1 Bonding

It is mandatory for the DT to support initiation of bonding, and for the GW to accept bonding.

7 REFERENCES

[1] TS 101 369 (GSM 07.10) version 6.1.0

[2] TIA-578-A Facsimile Digital Interface. Asynchronous Facsimile DCE Control Standard, Service Class 1

[3] TIA-592 Facsimile Digital Interface. Asynchronous Facsimile DCE Control Standard, Service Class 2

[4] ITU T.31 Asynchronous Facsimile DCE Control – Service Class 1

[5] ITU T.32 Asynchronous Facsimile DCE Control – Service Class 2

[6] International Telecommunication Union, “ITU-T Recommendation V.250”

8 LIST OF FIGURES

9 LIST OF TABLES

Part K:9

LAN ACCESS PROFILE

This document is a LAN Access Profile for Bluetooth devices. Firstly, this profile defines how Bluetooth-enabled devices can access the services of a LAN using PPP. Secondly, this profile shows how the same PPP mechanisms are used to form a network consisting of two Bluetooth-enabled devices.

CONTENTS

1 INTRODUCTION

1.1 SCOPE

This profile defines LAN Access using PPP over RFCOMM. There may be other means of LAN Access in the future.

- PPP is a widely deployed means of allowing access to networks. PPP provides authentication, encryption, data compression and multi-protocol facilities. PPP over RFCOMM has been chosen as a means of providing LAN Access for Bluetooth devices because of the large installed base of devices equipped with PPP software.
- It is recognized that PPP is capable of supporting various networking protocols (e.g. IP, IPX, etc.). This profile does not mandate the use of any particular protocol. However, since IP is recognized as the most important protocol used in today's networks, additional IP-related information is provided in an appendix. The use of these other PPP protocols is not discussed.
- This profile does not deal with conferencing, LAN emulation, ad-hoc networking or any other means of providing LAN Access. These functions are, or may be, dealt with in other Bluetooth profiles.

This profile defines how PPP networking is supported in the following situations.

a) LAN Access for a single Bluetooth device.

b) LAN Access for multiple Bluetooth devices.

c) PC to PC (using PPP networking over serial cable emulation).

1.2 PROFILE DEPENDENCIES

In Figure 1.1, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile does have dependencies – direct and indirect – on the profile(s) within which it is contained, as illustrated in the figure.
In particular, this LAN Access profile is dependent on the Serial Port and Generic Access profiles.

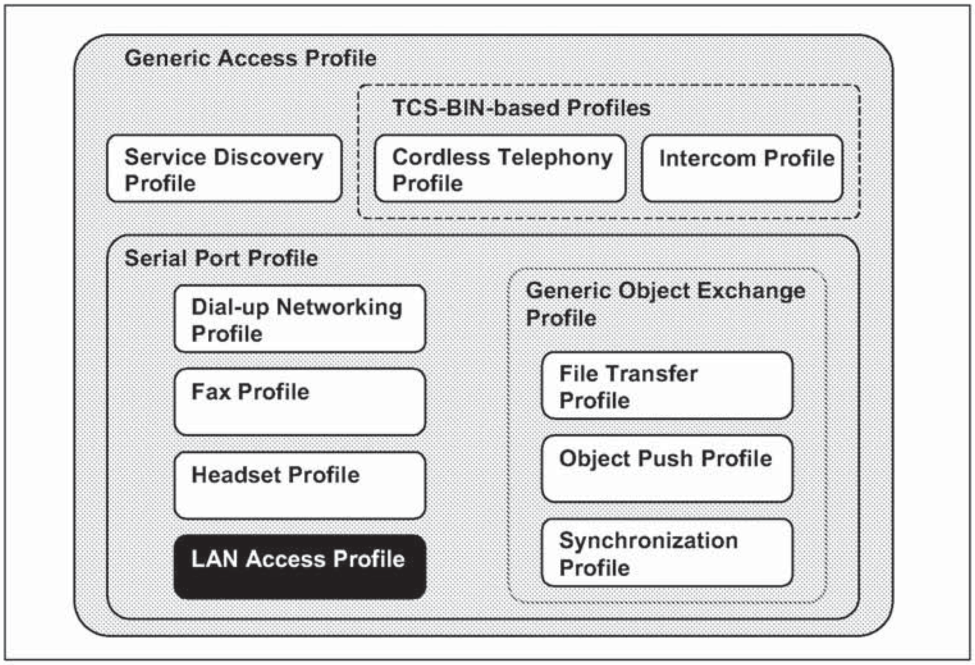

Figure 1.1: Bluetooth Profiles

1.3 SYMBOLS AND CONVENTIONS

This profile uses the symbols and conventions specified in Section 1.2 of the Generic Access Profile [13].

2 PROFILE OVERVIEW

2.1 PROTOCOL STACK

The figure below shows the protocols and entities used in this profile.

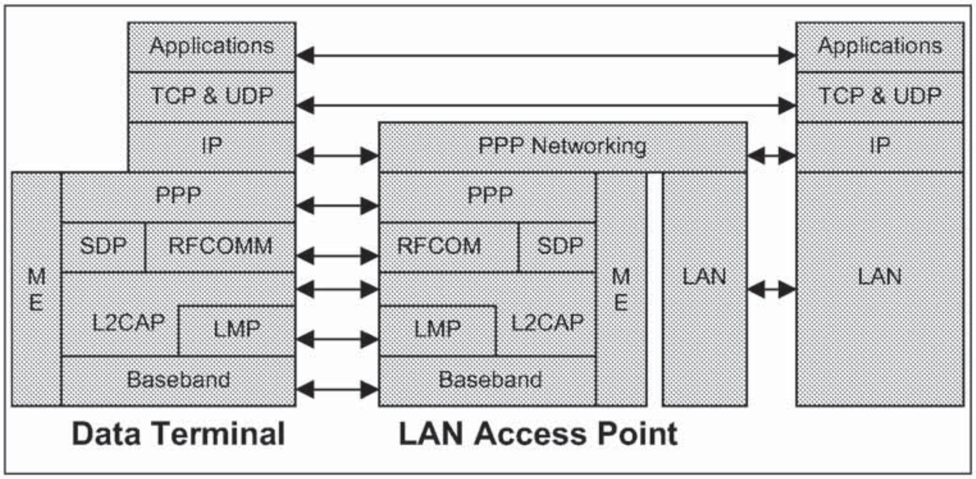

Figure 2.1: Protocol Stack

PPP is the IETF Point-to-Point Protocol [8]. PPP-Networking is the means of taking IP packets to/from the PPP layer and placing them onto the LAN. This mechanism is not defined by this profile but is a well-understood feature of Remote Access Server products.

The Baseband [1], LMP [2] and L2CAP [3] are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM [4] is the Bluetooth adaptation of GSM TS 07.10 [5]. SDP is the Bluetooth Service Discovery Protocol [6].

ME is the Management Entity which coordinates procedures during initialization, configuration and connection management.

2.2 CONFIGURATIONS AND ROLES

The following roles are defined for this profile.

LAN Access Point **(LAP) –** This is the Bluetooth device that provides access to a LAN (e.g. Ethernet, Token Ring, Fiber Channel, Cable Modem, Firewire, USB, Home Networking). The LAP provides the services of a PPP Server. The PPP connection is carried over RFCOMM. RFCOMM is used to transport the PPP packets and it can also be used for flow control of the PPP data stream.

Data Terminal **(DT)** – This is the device that uses the services of the LAP. Typical devices acting as data terminals are laptops, notebooks, desktop PCs and PDAs. The DT is a PPP client. It forms a PPP connection with a LAP in order to gain access to a LAN.

This profile assumes that the LAP and the DT each have a single Bluetooth radio.[1]

2.3 USER REQUIREMENTS AND SCENARIOS

The following scenarios are covered by this profile.

1. A single DT uses a LAP as a wireless means for connecting to a Local Area Network (LAN). Once connected, the DT will operate as if it were connected to the LAN via dial-up networking. The DT can access all of the services provided by the LAN.

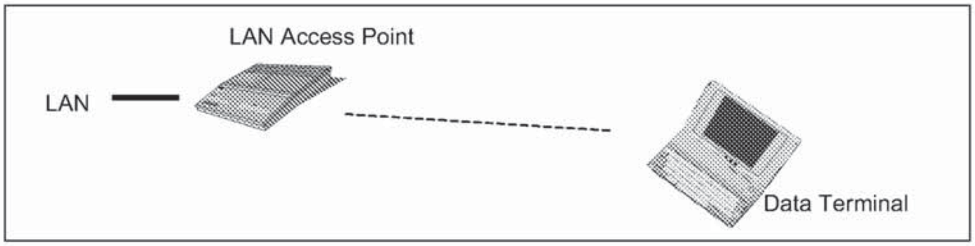

Figure 2.2: LAN Access by a single DT.

[1] Products with multiple radios can still conform to this profile. The LAP and DT roles can be adopted independently by each radio.

2. Multiple DTs use a LAP as a wireless means for connecting to a Local Area Network (LAN). Once connected, the DTs will operate as if they were connected to the LAN via dial-up networking. The DTs can access all of the services provided by the LAN. The DTs can also communicate with each other via the LAP.[2]

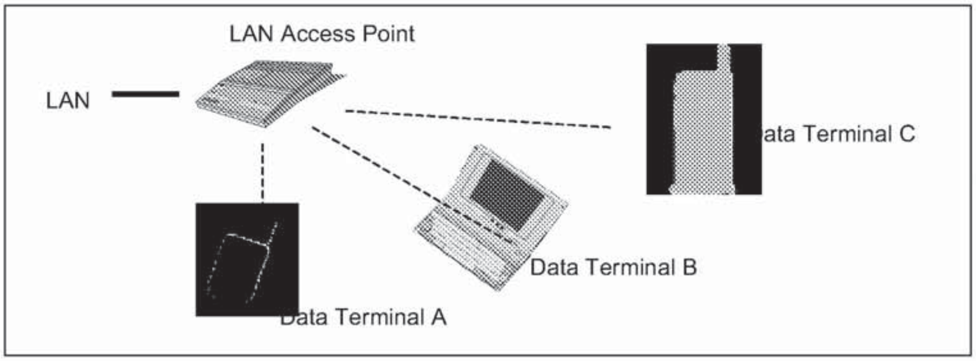

Figure 2.3: LAN Access by multiple DTs.

3. PC to PC connection. This is where two Bluetooth devices can form a single connection with each other. This scenario is similar to a direct cable connection commonly used to connect two PCs. In this scenario, one of the devices will take the role of a LAP, the other will be a DT. See Appendix 13.1 for more details of how this can be configured.

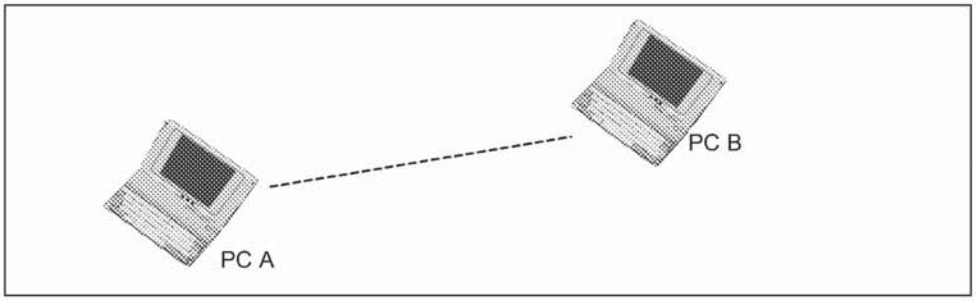

Figure 2.4: PC to PC connection.

Some LAP products may have an internal LAN or use the PSTN to access the Internet or corporate networks. The dial-up mechanisms to achieve the Internet connection are specific to the LAP. The DTs are totally unaware of these activities – except maybe in the event of longer connection times and traffic delays.

[2] The DTs will be able to communicate with each other only if the required services (e.g. DNS) are available on the LAN.

2.4 PROFILE FUNDAMENTALS

Here is a brief summary of the interactions between a DT and a LAP. Subsequent sections in this profile provide more detail for each of the following steps.

1. The first step is to find a LAP that is within radio range and is providing a PPP/RFCOMM/L2CAP service. For example, the DT user could use some application to find and select a suitable LAP.
2. If there is no existing baseband physical link, then the DT requests a baseband physical link with the selected LAP. At some point after the physical link establishment, the devices perform mutual authentication. Each device insists that encryption is used on the link – see Section 3.1.
3. The DT establishes a PPP/RFCOMM/L2CAP connection.
4. Optionally, the LAP may use some appropriate PPP authentication mechanism (e.g. CHAP [21]). For example, the LAP may challenge the DT's user to authenticate himself or herself; the DT must then supply a username and password. If these mechanisms are used and the DT fails to authenticate itself, then the PPP link will be dropped.
5. Using the appropriate PPP mechanisms, a suitable IP address is negotiated between the LAP and the DT.
6. IP traffic can now flow across the PPP connection.
7. At any time the DT or the LAP may terminate the PPP connection.

2.5 CONFORMANCE

If conformance to this profile is claimed, all capabilities indicated mandatory for this profile shall be supported in the specified manner (process-mandatory). This also applies to all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth certification program.

3 USER INTERFACE ASPECTS

This profile is built upon the Generic Access Profile.

- When reading Generic Access Profile, DevA (the connection initiator) is equivalent to DT, and DevB is equivalent to the LAP.
- All the mandatory requirements defined in Generic Access Profile are mandatory for this profile.
- Unless otherwise stated below, all the optional requirements defined in Generic Access Profile are optional for this profile.

3.1 SECURITY

It is recognized that security in a wireless environment is of paramount importance.

Both the LAP and the DT must enforce that encryption is operating on the baseband physical link while any PPP traffic is being sent or received. The LAP and the DT will refuse any request to disable encryption. Therefore, Bluetooth pairing must occur as a means of authenticating the users. A PIN or link key must be supplied, even if the default PIN is used. The default PIN for LAN access is a zero length PIN. Failure to complete the pairing process will prevent access to the LAN Access service.

A more sophisticated product may require further authentication, encryption and/or authorization.

3.2 GENERIC MODES

The following modes are defined in Section 4 of Generic Access Profile [13]. This profile requires the following support.

Modes	Support in LAP	Support in DT
Discoverability modes		
Non-discoverable mode	O	X
Limited discoverable mode	X	X
General discoverable mode	M	X
Connectability modes		
Non-connectable mode	O	X
Connectable mode	M	X
Pairing modes		
Non-pairable mode	O	X
Pairable mode	M	X

Table 3.1: Generic Mode requirements table

Notes

1. A typical use for the Non-discoverable mode is where the LAP is intended for personal use only. The DT would remember the identity of the LAP and never need to use the Bluetooth inquiry mechanism.
2. A typical use for the General discoverable mode is where the LAP is intended for general use. The DT would not be expected to remember the identity of all the LAPs that it uses. The DT is expected to use the Bluetooth inquiry mechanism to discover the LAPs in range.

3.3 ADDITIONAL PARAMETERS

The following parameter is mandatory for the LAP. Optionally it may be configurable by the LAP administrator.

Maximum number of users. Different products have different capabilities and resource limitations that will limit the number of simultaneous users that they can support. The administrator of the LAP may choose to further limit the number of simultaneous users.[3]

- **Single-user mode** is when the maximum number of users is configured to allow only a single user. In this mode, either the DT or the LAP may be the master of the piconet. Single-user mode means that a single DT has exclusive access to a LAP.[4]
- **Multi-user mode** is when the maximum number of users is configured to allow more than one user. In this mode, the LAP must always become the master of the piconet. If the DT refuses to allow the LAP to become master, then the DT cannot gain access to the LAN.

[3] The fewer simultaneous users there are using a Bluetooth radio, the more bandwidth will be available to each. A LAP can be restricted to a single user.

[4] There are situations where a DT may wish to connect to a LAP and still remain the master of an existing piconet. For example, a PC is the master of a piconet with connections to a Bluetooth mouse and a Bluetooth video projector. The PC then requires a connection to the LAP, but must remain master of the existing piconet. If, for some reason, the PC can only be a member of one piconet, then the LAP must be a piconet slave. This situation is only possible if the LAP's 'maximum number of users' parameter has been configured to 1; i.e. single-user mode.

4 APPLICATION LAYER

Section	Feature	Support in LAP	Support in DT
4.1	Initialization of LAN Access service	M	X
4.2	Shutdown of LAN Access service	M	X
4.3	Establish LAN Connection	C1	M
4.4	Lost LAN Connection	X	M
4.5	Disconnect LAN Connection	M	M

Table 4.1: Application-layer requirements table

C1: Currently the LAP is not required to initiate a LAN connection establishment. In the future, a LAP may initiate a connection (e.g. as part of some form of LAP-initiated hand-off).

4.1 INITIALIZATION OF LAN ACCESS POINT SERVICE

This procedure initiates the configuration of the device as a LAP. This operation involves setting the following parameters:

- All the configurable parameters defined in Section 3.2. (For example, maximum number of users, discoverability mode, etc.)
- The required Bluetooth PINs and/or link keys.
- Any appropriate PPP configuration options (e.g. authentication, compression) can be configured. In order to ensure interoperability, a LAP shall not require connecting DTs to perform any PPP authentication, until the LAP administrator has configured PPP authentication.

When initialization is complete, the device will be able to accept PPP connections.

For products whose main role is that of a LAP, this initialization procedure is typically run automatically when the device is powered up.

For other products (e.g. PCs, Notebooks, etc.), this initialization procedure allows the user to configure the product as an access point, so that a DT can connect to it.

4.2 SHUTDOWN OF LAN ACCESS POINT SERVICE

This procedure stops the device from acting as a LAP.

- The PPP Server is shutdown – as defined in Section 5.2.
- Optionally, a product may take steps to prevent un-authorized Bluetooth access at a later time by deleting some of the stored link keys.

4.3 ESTABLISH LAN CONNECTION

Normally the DT will initiate the establishment of a connection to the LAN.

1. The first step is to select a LAP and a suitable PPP/RFCOMM service that it provides. This selection may be done in one of the following ways:

- The DT user is presented with a list of LAPs that are within radio range, and the services that they provide. The user can then select a LAP/service from the list provided.
- The DT user is presented with a list of services that are being provided by the LAPs that are within radio range. Where the same service is provided by multiple LAPs (i.e. identical ServiceClass-IDs), the application may choose to show the service only once. The user can then select a service from the list provided. The DT will automatically select a suitable LAP that provides the selected service.
- The DT user enters the name of the service that is required, e.g. 'network', or 'Meeting #1' (see Section 7.1 for more information on service names). The DT will automatically select a suitable LAP that provides the required service.
- Some application on the DT automatically searches for and selects a suitable LAP/service.

Whatever means is used, the result of the selection process must be a LAP that is within radio range and a PPP/RFCOMM service that it provides.

In all cases, the Bluetooth Service Discovery mechanisms are used to retrieve service information. This service information provides all the information required to create the RFCOMM connection in step 4.

2. Optionally, the DT user (or application) is allowed to enter a Bluetooth Authentication PIN or link key supplied by the application. If no PIN is entered, then a zero-length PIN is used.
3. Optionally, the DT user (or application) is allowed to enter a username and password for PPP authentication. If some PPP authentication mechanism is used and the user does not initially supply the username and password, then he/she may be prompted for them later in the connection establishment.

4. When the user (or application) activates the connection, then a PPP application is started, to attempt to establish a connection to the selected access point/service using the procedures in 12.1.

More complex situations (e.g. hand-off of a DT between LAPs) may require the LAP to initiate the establishment of a connection. These situations are possible, but are outside the scope of this document.

4.4 LOST LAN CONNECTION

If the LAN connection is lost for any reason, then the DT user (or application) must be notified of connection failure.

Optionally, the application may allow re-establishment of the connection to the same (or similar) LAP/service. The application could remember the previous LAP, service, PIN, link key, username and password and use them to allow speedy or automatic re-establishment of the LAN connection. The procedures described in Section 5.1 will be used.

4.5 DISCONNECT LAN CONNECTION

Either the LAP or the DT may terminate the LAN Connection at any time – using the procedures in Section 5.4.

5 PPP

PPP/RFCOMM operation in this profile is similar to PPP operation in normal dial-up networking, except that this profile omits the use of AT commands; PPP starts as soon as the RFCOMM link is established. By contrast, in dial-up networking, AT commands are used to establish the link, then PPP starts communicating.

The LAP exports a PPP Server interface [8]. This specification does not require any particular means of achieving the 'appearance' of a PPP Server. One implementation of a LAP could contain a PPP Server. Alternatively, the LAP could be some kind of PPP proxy, where PPP packets are transferred to/from a PPP server somewhere else on the network.

The following text, together with the associated sub-clauses, defines the mandatory requirements with regard to this profile.

Section	Procedure	Support in LAP	Support in DT
5.1	Initialize PPP	M	X
5.2	Shutdown PPP	M	X
5.3	Establish PPP Connection	M	M
5.4	Disconnect PPP Connection	M	M
5.5	PPP Authentication Protocols	O	O

Table 5.1: PPP capabilities

5.1 INITIALIZE PPP

On the LAP, the existence of a PPP Server shall be registered in the Service Discovery Database. The service attributes are defined in 7.1.

A device in the DT role does not register PPP in the Service Discovery Database. However, it is possible for a device to be both a LAP and a DT; therefore the device could register PPP in the Service Discovery Database as defined above.

PPP is a packet-oriented protocol, whereas RFCOMM expects serial data streams. Therefore, the PPP layer must use the serialization mechanisms described in [9].

5.2 SHUTDOWN PPP

All existing PPP connections are disconnected.

The PPP layer disables or removes the PPP service entry from the Service Discovery Database.

5.3 ESTABLISH PPP CONNECTION

If there is no existing RFCOMM session between the LAP and the DT, then the device initiating the PPP connection shall first initialize RFCOMM (see Section 6). The device obtains the RFCOMM Server channel to use from the service information it discovered earlier.

Using the Link Control Protocol (LCP) [8], the LAP and DT negotiate a PPP link.

Part of the LCP is the negotiation of the Maximum Transmission Unit (MTU) to be used on the PPP link – see [8] for details. This profile places no requirements on the negotiated MTU.[5]

Depending upon its capabilities and configuration (see 3.2), a LAP may have multiple PPP sessions in operation simultaneously.

5.4 DISCONNECT PPP CONNECTION

The following reasons will cause PPP to terminate the connection:

1. User intervention.
2. Failure of the RFCOMM/L2CAP connection. The RFCOMM/L2CAP connection may fail for several reasons. For example, when the radio link has failed or the device has been out of range for an excessive amount of time; see [3].
3. Termination by the LAP, if the access point can no longer provide the appropriate service. The reasons that would cause this are very dependent on the implementation of the LAP, but they could include (a) detection of duplicate IP addresses, (b) loss of connection to the LAN, (c) loss of connectivity to the PPP Server, or (d) loss of connection to the required IP subnet.
4. Some implementation-specific policy decision made by an application that is running on the LAP or the DT.

PPP handles each of the above situations differently. Reasons 1, 3 and 4 above result in a controlled disconnection at each protocol layer. Reason 2 above requires different processing.

[5] Some products may use the LCP negotiation process to insist on specific values for the MTU. For example, a simple LAP with an Ethernet connection may wish to have a suitable MTU, so that IP packets do not require fragmentation when transmitted from Bluetooth to Ethernet.

When the PPP connection is terminated, either by user intervention or automatically by the LAP, then the PPP layer takes the following steps:

1. Gracefully terminate the IPCP connections (as defined in [24]). This will cause the IP interface to be disabled.
2. Gracefully terminate the LCP connections (as defined in [8]),
3. Disconnect the RFCOMM connection (as defined in Serial Port Profile)

When the RFCOMM/L2CAP connection suddenly terminates, then the PPP layer takes the following steps:

1. Terminate the IPCP connections (as defined in [24]). This will cause the IP interface to be disabled.
2. Terminate the LCP connections (as defined in [8]).

5.5 PPP AUTHENTICATION PROTOCOLS

Optionally, a LAP may be configured to use one or more of the PPP authentication protocols. These protocols allow a network administrator to control access to the network. The use of these PPP protocols does not form part of this profile. They are mentioned here for information only.

PPP supports a number of authentication protocols including the following:

- PPP Challenge Handshake Authentication Protocol (CHAP) [21]
- Microsoft PPP CHAP Extensions [22]
- PPP Authentication [23]
- PPP Extensible Authentication Protocol (EAP) [23]

Typically, the user needs to supply a username and password in order to gain authorization to use the PPP connection. If the authentication fails, then the PPP connection is normally dropped.

The PPP authentication protocols are independent of the Bluetooth authentication mechanisms. A network administrator may choose to use any combination of the PPP and Bluetooth mechanisms.

6 RFCOMM

This section describes the requirements on RFCOMM in units complying with the LAN Access Profile.

This profile is built upon the Serial Port Profile [10]. The requirements defined in the Serial Port Profile Section 4, "RFCOMM Interoperability Requirements," on page 177, apply to this profile.

- When reading [10], DevA (the connection initiator) is equivalent to DT and DevB is equivalent to the LAP.
- All the mandatory requirements defined in the Serial Port Profile Section 4 on page 177 are mandatory for this profile.
- All the optional requirements defined in the Serial Port Profile Section 4 on page 177 are optional for this profile.

In addition:

1. In order to maximize packet throughput, it is recommended that RFCOMM should make use of the 3 and 5 slot baseband packets.
2. As defined in [4] section 2, the speed of RFCOMM connections is not configurable by the user. RFCOMM will transfer the data as fast as it can. The actual transfer rate will vary, depending upon the other Bluetooth traffic on the baseband link. In particular, the connection speed will <u>not</u> be artificially held at some typical serial port value; e.g. 19200.

7 SERVICE DISCOVERY

A LAP will be capable of providing one or more services for connecting to a LAN. For example, different services could provide access to different IP subnets on the LAN. The DT's user must be able to choose which of the LAN access services he or she requires.

7.1 SDP SERVICE RECORDS

Each LAP will provide one Service Class for PPP/RFCOMM services. A LAP may contain multiple instances of this Service Class; e.g. access to multiple subnets. Where the access point provides more than one PPP/RFCOMM service, the service selection is based on service attributes. These services are made public via the SDP.

The service record will have the following attributes. The syntax and usage of these attributes is defined in [6].

Item	Definition	Mand. /Opt.	Type	Value	Default Value
ServiceClassIDList		Mand.			
ServiceClass0	UUID for "LAN Access using PPP"	Mand.	UUID	See [11]	See [11]
ProtocolDescriptorList		Mand.			
Protocol0	UUID for L2CAP protocol	Mand.	UUID	See [11]	See [11]
Protocol1	UUID for RFCOMM protocol	Mand.	UUID	See [11]	See [11]
Parameter0	Server channel	Mand.	UInt8	varies	varies
ProfileDescriptorList		Opt.			
Profile #0	Uuid for "LAN Access using PPP"		UUID	see [11]	see [11]
Parameter0	Version "1.00"		Uint16	0x0100	0x0100
ServiceName	Displayable name	Opt.	String	Configurable	'LAN Access using PPP'
ServiceDescription	Displayable Information	Opt.	String	Configurable	'LAN Access using PPP'
ServiceAvailability	Load Factor	Opt.	Uint8	Dynamic	Dynamic
IpSubnet	Displayable Information	Opt.	String	Configurable	Configurable

The actual values of universal attribute IDs are defined in the Assigned Numbers specification [11] section 4. Values that are of the type UUID are defined in the Assigned Numbers specification [11] section 4.

- The ServiceName attribute is a short user-friendly name for the service; e.g. 'Corporate Network', 'Conference#1', etc.
- The ServiceDescription attribute is a longer description of the service. For example. "This network is provided for our guests. It provides free Internet Access and printing services. No username or password are required."
- The ServiceAvailability attribute may be used in conjunction with the Load-Factor field of the CoD defined for LAN Access Points – see [11] section 1.2.6.
- The IpSubnet attributeID is (0x0200). This attribute is a displayable string containing subnet definition of the network, e.g. "191.34.12.0/24". The first 4 numbers define the IP subnet in dotted-decimal notation. The fifth number, after the "/" character, is the number of subnet bits to use in the subnet mask; e.g. 24 means a subnet mask of 255.255.255.0.

8 L2CAP

This section describes the requirements on L2CAP in units complying with the LAN Access Profile.

This profile is built upon the Serial Port Profile [10]. The requirements defined in the Serial Port Profile Section 5, "L2CAP Interoperability Requirements," on page 179 apply to this profile.

- When reading [10], DevA (the connection initiator) is equivalent to DT and DevB is equivalent to the LAP.
- All the mandatory requirements defined in the Serial Port Profile section 5 on page 179 are mandatory for this profile.
- All the optional requirements defined in the Serial Port Profile Section 5 on page 179 are optional for this profile.

In addition:

1. The MTU used at the L2CAP layer is determined by the RFCOMM parameter 'maximum frame size' – see Section 6 on page 284.

9 LINK MANAGER

This section describes the requirements on Link Manager in units complying with the LAN Access Profile.

This profile is built upon the Serial Port Profile [10]. The requirements defined in the Serial Port Profile Section 7, "Link Manager (LM) Interoperability Requirements," on page 183 apply to this profile.

- When reading [10], DevA (the connection initiator) is equivalent to DT and DevB is equivalent to the LAP.
- All the mandatory requirements defined in the Serial Port Profile Section 7 on page 183 are mandatory for this profile.
- The following optional requirements defined in the Serial Port Profile Section 7 on page 183 are mandatory for this profile.

Procedure	Support in LAP	Support in DT
Authentication	M	M
Pairing	M	M
Encryption	M	M
Request master/slave switch	M	X
Perform master/slave switch	M	M

Table 9.1: LMP procedures

- All the remaining optional requirements defined in the Serial Port Profile Section 7 on page 183 are optional for this profile.

In addition:

- For bandwidth reasons, it is advisable but not mandatory for both devices to use multi-slot packets.
- When the LAP is configured in single-user mode (i.e. maximum number of users is 1), then the LAP may be either the master or the slave of the piconet.
- When the LAP is configured in multi-user mode (i.e. maximum number of users is more than 1), then the LAP must be the master of the piconet.

9.1 PROFILE ERRORS

The LAP must deny access to the PPP service if the DT fails to comply with the requirements of this profile, as follows:

1. Failure to complete the pairing process.
2. Failure to comply with a request to enable encryption on the baseband connection.
3. Failure by the DT to comply with a request to perform a master/slave switch. The LAP only requests a master/slave switch when it is configured in multi-user mode. In this mode the LAP must be the master of the piconet.

The LAP must reject all attempts by the DT to perform the following operations (see [2] section 5.1.2 for the appropriate LMP rejection reasons):

4. Requesting that encryption be disabled. The error code “Host Rejected due to security reasons” is used.
5. Requesting that the LAP switch to be a slave when the LAP is configured to be in multi-user mode. The error code “Unspecified Error” is used.
6. Requesting that a new connection be made when the LAP already has its configured maximum number of users. The error code “Other End Terminated Connection: Low Resources” is used.

10 LINK CONTROL

This section describes the requirements on Link Control in units complying with the LAN Access Profile.

This profile is built upon the Serial Port Profile [10]. The requirements defined in the Serial Port Profile, Section 8, "Link Control (LC) Interoperability Requirements," on page 184, apply to this profile.

- When reading [10], DevA (the connection initiator) is equivalent to DT and DevB is equivalent to the LAP.
- All the mandatory requirements defined in the Serial Port Profile, Section 8 on page 184, are mandatory for this profile.
- All the optional requirements defined in the Serial Port Profile, Section 8 on page 184, are optional for this profile.
- The timer definitions defined in the Serial Port Profile, Section 8 on page 184, are not used in this profile.

In addition:

1. The Non-discoverable and General Discoverable Modes of the LAP (i.e. how InquiryScan is used) are defined in the Generic Access Profile [13], Section 4 on page 29.
2. In order to discover the nearby LAPs, a DT must use the General Inquiry procedure defined in the Generic Access Profile [13], Section 6 on page 37.

11 MANAGEMENT ENTITY PROCEDURES

The following text together with the associated sub-clauses defines the mandatory requirements with regard to this profile.

Section	Procedure	Support in LAP	Support in DT
11.1	Link Establishment	M	M
11.2	Single/Multi-user mode	M	N/A

Table 11.1: Management Entity Procedures

11.1 LINK ESTABLISHMENT

Link Establishment is required for communication between a LAP and a DT. The Link Establishment procedure is started as a direct consequence of the user operations described in "Establish LAN Connection" Section 4.3.

1. The DT first performs a General Inquiry to discover what LAPs are within radio range, see Generic Access Profile, Section 6 on page 37. Having performed the inquiry, the DT will have gathered a list of responses from nearby LAPs.
2. The DT sorts the list according to some product-specific criteria. The LAN Access Point CoD contains a field called 'Load Factor', see [11] section 1.2.6. It is recommended (but not mandated) that this field is used to sort the list.
3. The DT shall start with the LAP at the top of the list and try to establish a link with it, see Generic Access Profile, Section 7.1 on page 45. Any error or failure to establish a link shall cause the DT to skip this LAP. The DT will attempt to establish a link the next LAP in the list.
4. If there are no more LAPs in the list, the DT shall not proceed with further link establishment procedures. Link establishment has to be re-initiated.

The following subsections apply.

11.1.1 No responses to inquiry

If the DT did not get any response during inquiry, the DT shall not proceed with further link establishment procedures. Link establishment has to be re-initiated by the user or an application.

11.1.2 No response to paging

If a LAP does not respond to paging attempts, the DT shall skip this LAP.

11.1.3 Pairing

During link establishment, the LAP and DT are paired, which means that the DT and LAP build a security wall towards other devices.

11.1.4 Errors

If any LM procedure or Service Discovery procedure fails, or if link is lost at any time during link establishment, then the DT shall skip this LAP.

11.2 MAXIMUM NUMBER OF USERS

When the LAP is configured to allow multiple users, then the LAP must be the master of the piconet, see 3.2. In this mode, the Management Entity on the LAP ensures that the LAP remains the master of the Bluetooth piconet.

While in multi-user mode, the LAP shall request that it become the master of any new baseband physical link. If, for any reason, the LAP cannot remain the master, then the baseband physical link shall fail. The LMP [2] allows a device to (a) request a master/slave switch, and also (b) to refuse to comply with a request to perform a master/slave switch, see [1] section 10.9.3.

12 APPENDIX A (NORMATIVE): TIMERS AND COUNTERS

No specific timers are required by this profile.

Timer name	Recommended value	Description	Comment

Table 12.1: Defined timers

No specific counters are required by this profile.

Counter name	Proposed value	Description	Comment

Table 12.2: Defined Counters

The following parameters are required by this profile.

Parameter	Description
Discoverability mode	Controls whether the DT can discover the LAP.
Connectability mode	Controls whether the DT can be connected to the LAP.
Pairing mode	Controls whether the DT can be pair with the LAP.
Maximum users	The maximum the number of simultaneous users/connections.

Table 12.3: Defined parameters

13 APPENDIX B (NORMATIVE): MICROSOFT WINDOWS

This section contains various bits of information relating to Microsoft Windows and how it can be used in this profile.

13.1 PC-2-PC CONFIGURATION

This section contains information for configuring two PCs to form a connection. This configuration is independent of Bluetooth. This configuration is the same whether a serial cable or Bluetooth is used to make the connection.

- It is known that Windows '98 comes with a PPP server and that this PPP Server can be used to achieve the PC-to-PC feature. Detailed configuration information is available at the following Web sites.

  Microsoft Direct Cable Connection & Dial-up networking:

  http://support.microsoft.com/support/windows/ServiceWare/

  Win95/33BKKC22.ASP

  http://www.wown.com/

  http://www.tecno.demon.co.uk/dcc.html

  http://www.cs.purdue.edu/homes/kime/directcc/directcc95.htm

- This application requires some exchange of text strings before the PPP connection will become operational. The client PC sends the string 'CLIENT' and the server must reply with 'CLIENTSERVER'.
- The tools provided by Windows '98 configure one PC as the server and the other as the client. The PC configured as the server can share its resources with the client, but not vice versa.

14 APPENDIX C (INFORMATIVE): INTERNET PROTOCOL (IP)

The use of IP in this profile is optional. This section is provided for information only.

This section contains various bits of IP information that relate to various parts of this profile.

14.1 IP INTERFACES

14.1.1 Interface Enabled

The PPP layer in the DT will enable an IP interface when the IPCP link has been established and a suitable IP address has been negotiated. Typically, the DT will only have one PPP session in operation and only need one IP interface.

The DT may also need to configure its default gateway – WINS, DNS, etc. This profile does not define how this configuration is achieved. Mechanisms exist within PPP for supplying this information, see [24]. Other mechanisms may be used as appropriate.

In the event a DT has multiple IP interfaces, we rely on the IP protocol layer within the DT to select the correct interface to use for transmitting packets.

14.1.2 Interface Disabled

When the PPP connection is terminated or aborted, then the IP interface is disabled. The IP protocol stack will then remove that IP address from its routing tables.

14.2 THE IPCP PROTOCOL

Optionally, a LAP may be configured to support the IP protocol. The use of this PPP protocol does not form part of this profile. It is mentioned here for information only.

If supported, the IPCP protocol must be fully supported as defined in [24].

The following sub-sections concerning IPCP are informational only. They briefly describe certain aspects of IPCP. See [24] for full details.

14.2.1 IPCP Connection

IPCP only starts to operate after (a) the PPP connection has been established using LCP and optionally (b) the user has been authenticated.

The IPCP protocol negotiates certain parameters between the LAP and the DT.

Once the IPCP connection is established, and a suitable IP address has been negotiated, then IP interface is enabled.

14.2.2 IP Address Allocation

The DT will require an IP address in order to operate on the LAN. Current PPP implementations allow only three possibilities:

1. The IPCP option is used to specify a pre-configured IP address. If this IP address is not suitable on the LAN, then the IPCP link will not be established.
2. The IPCP option is used to request a suitable IP configuration from a PPP Server.
3. The IPCP Mobile-IP options are used to request a specified IP configuration. When moving between access points on the same LAN, it may be advantageous for the DT to continue using the same IP configuration.

14.2.3 DNS and NBNS addresses

Optionally, the LAP support could include the IPCP extensions defined in RFC1877 (defined by Microsoft). These extensions define the negotiation of primary and secondary Domain Name System (DNS) and NetBIOS Name Server (NBNS) addresses.

14.2.4 NetBIOS over IP

The NetBIOS protocol is used by Microsoft Windows to implement many of its networking features. The NetBIOS protocol can be carried over IP packets as defined in [29] and [30].

15 LIST OF FIGURES

16 LIST OF TABLES

17 REFERENCES

17.1 NORMATIVE REFERENCES

[1] Bluetooth Baseband specification (See Volume 1, Part B)

[2] Bluetooth Link Manager Protocol (See Volume 1, Part C)

[3] Bluetooth Logical Link Control and Adaptation Protocol Specification (See Volume 1, Part D)

[4] RFCOMM with TS 07.10 (See Volume 1, Part F:1)

[5] TS 101 369 (GSM 07.10) version 6.2.0.

[6] Bluetooth Service Discovery Protocol (SDP) (See Volume 1, Part E)

[7] John Webb, "Bluetooth SIG MRD", version 1.0.

[8] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 50, RFC 1661, Daydreamer, July 1994.

[9] Simpson, W., Editor, "PPP in HDLC Framing", STD 51, RFC 1662, Daydreamer, July 1994.

[10] Serial Port Profile

[11] Bluetooth Assigned Numbers (See Volume 1,Appendix VIII)

[12] Thomas Muller, “Bluetooth Security Architecture”. Version 1.0.

[13] Generic Access Profile

17.2 INFORMATIVE REFERENCES

[20] Lloyd, B., and W. Simpson, "PPP Authentication Protocols", RFC 1334, Lloyd Internetworking, Daydreamer, October 1992.

[21] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[22] Zorn, G., " Microsoft PPP CHAP Extensions", RFC 2433, October 1998.

[23] L. Blunk., " PPP Extensible Authentication Protocol (EAP)", RFC 2433, March 1998.

[24] McGregor, G., " The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[25] Simpson, W., " The PPP Internetwork Packet Exchange Control Protocol (IPXCP)", RFC 1552, December 1993.

[26] Pall, G., " The PPP NetBIOS Frames Control Protocol (NBFCP)”, RFC 2097, January 1997.

[27] " Mobile-IPv4 Configuration Option for PPP IPCP ", RFC 2290.

[28] Cobb, S., " PPP Internet Protocol Control Protocol Extensions for Name Server Addresses”, RFC 1877, December 1995.

[29] NetBIOS Working Group, “PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS”, RFC 1001, March 1987.

[30] NetBIOS Working Group, “PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS”, RFC 1002, March 1987.

Part K:10

GENERIC OBJECT EXCHANGE PROFILE

This profile defines the requirements for Bluetooth devices necessary for the support of the object exchange usage models. The requirements are expressed by defining the features and procedures that are required for interoperability between Bluetooth devices in the object exchange usage models.

CONTENTS

FOREWORD

The purpose of this document is to work as a generic profile document for all application profiles using the OBEX protocol.

Interoperability between devices from different manufacturers is provided for a specific service and usage model if the devices conform to a Bluetooth SIG defined profile specification. A profile defines a selection of messages and procedures (generally termed *capabilities*) from the Bluetooth SIG specifications and gives an unambiguous description of the air interface for specified service(s) and usage model(s).

All defined features are process-mandatory. This means that if a feature is used, it is used in a specified manner. Whether the provision of a feature is mandatory or optional is stated separately for both sides of the Bluetooth air interface.

1 INTRODUCTION

1.1 SCOPE

The Generic Object Exchange profile defines the protocols and procedures that shall be used by the applications providing the usage models which need the object exchange capabilities. The usage model can be, for example, Synchronization, File Transfer, or Object Push model. The most common devices using these usage models can be notebook PCs, PDAs, smart phones, and mobile phones.

1.2 BLUETOOTH PROFILE STRUCTURE

In Figure 1.1, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure: a profile has dependencies on the profile(s) in which it is contained – directly and indirectly. For example, the Object Push profile is dependent on Generic Object Exchange, Serial Port, and Generic Access profiles.

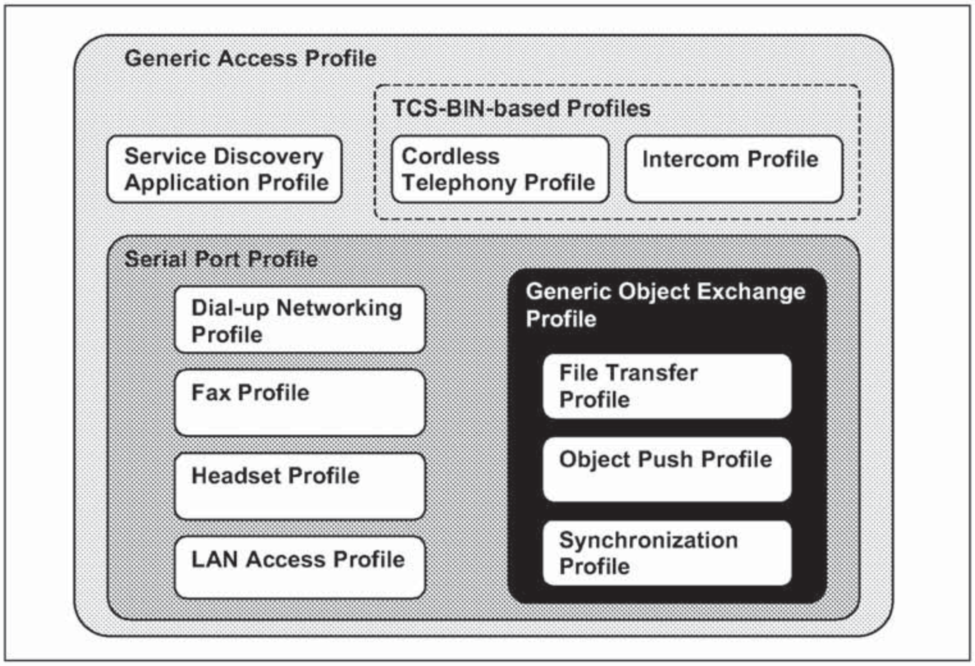

Figure 1.1: Bluetooth Profiles

1.3 BLUETOOTH OBEX-RELATED SPECIFICATIONS

Bluetooth Specification includes five separate specifications for OBEX and applications using it.

1. Bluetooth IrDA Interoperability Specification [1]

- Defines how the applications can function over both Bluetooth and IrDA.
- Specifies how OBEX is mapped over RFCOMM and TCP.
- Defines the application profiles using OBEX over Bluetooth.

2. Bluetooth Generic Object Exchange Profile Specification (This specification)

- Generic interoperability specification for the application profiles using OBEX.
- Defines the interoperability requirements of the lower protocol layers (e.g. Baseband and LMP) for the application profiles.

3. Bluetooth Synchronization Profile Specification [2]

- Application Profile for the Synchronization applications.
- Defines the interoperability requirements for the applications within the Synchronization application profile.
- Does not define the requirements for the Baseband, LMP, L2CAP, or RFCOMM.

4. Bluetooth File Transfer Profile Specification [3]

- Application Profile for the File Transfer applications.
- Defines the interoperability requirements for the applications within the File Transfer application profile.
- Does not define the requirements for the Baseband, LMP, L2CAP, or RFCOMM.

5. Bluetooth Object Push Profile Specification [4]

- Application Profile for the Object Push applications.
- Defines the interoperability requirements for the applications within the Object Push application profile.
- Does not define the requirements for the Baseband, LMP, L2CAP, or RFCOMM.

1.4 SYMBOLS AND CONVENTIONS

1.4.1 Requirement status symbols

In this document, the following symbols are used:

'M' for mandatory to support (used for capabilities that shall be used in the profile);

'O' for optional to support (used for capabilities that can be used in the profile);

'C' for conditional support (used for capabilities that shall be used in case a certain other capability is supported);

'X' for excluded (used for capabilities that may be supported by the unit but shall never be used in the profile);

'N/A' for not applicable (in the given context it is impossible to use this capability).

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices following this profile. Therefore, these features shall never be activated while a unit is operating as a unit within this profile.

1.4.2 Signaling diagram conventions

The following arrows are used in diagrams describing procedures:

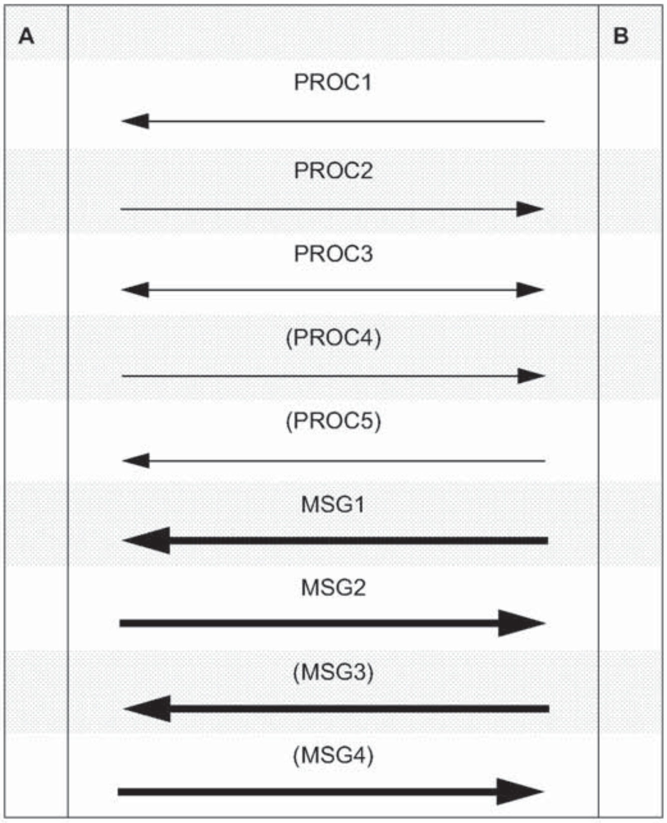

Table 1.1: Arrows used in signaling diagrams

In the table above, the following cases are shown: PROC1 is a sub-procedure initiated by B. PROC2 is a sub-procedure initiated by A. PROC3 is a sub-procedure where the initiating side is undefined (may be both A and B). PROC4 indicates an optional sub-procedure initiated by A, and PROC5 indicates an optional sub-procedure initiated by B.

MSG1 is a message sent from B to A. MSG2 is a message sent from A to B. MSG3 indicates an optional message from A to B, and MSG4 indicates an optional message from B to A.

2 PROFILE OVERVIEW

2.1 PROFILE STACK

The figure below shows the protocols and entities used in this profile.

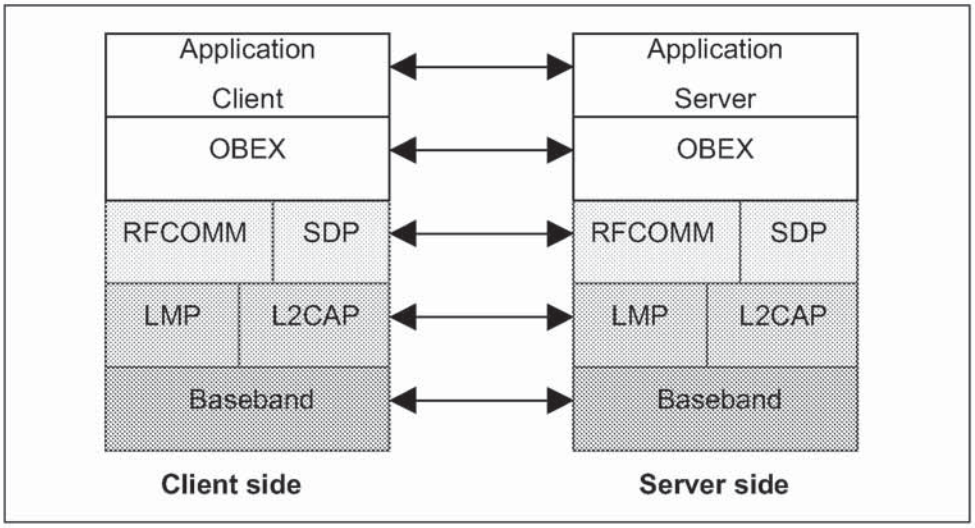

Figure 2.1: Protocol model

The Baseband [5], LMP [6] and L2CAP [7] are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM [8] is the Bluetooth adaptation of GSM TS 07.10 [9]. SDP is the Bluetooth Service Discovery Protocol [10]. OBEX [1] is the Bluetooth adaptation of IrOBEX [11].

The Application Client layer shown in Figure 2.1 is the entity sending and retrieving data object from the Server using the OBEX operations. The application Server is the data storage to and from which the data object can be sent or retrieved.

2.2 CONFIGURATIONS AND ROLES

The following roles are defined for this profile:

Server – This is the device that provides an object exchange server to and from which data objects can be pushed and pulled, respectively.

Client – This is the device that can push or/and pull data object(s) to and from the Server.

2.3 USER REQUIREMENTS AND SCENARIOS

The scenarios covered by this profile are the following:

- Usage of a Server by a Client to push data object(s)
- Usage of a Server by a Client to pull data object(s)

The following restrictions apply to this profile:

a) For the device containing the Server, it is assumed that the user may have to put it into the discoverable and connectable modes when the inquiry and link establishment procedures, respectively, are processed in the Client (see Generic Access Profile).

b) The profile only supports point-to-point configurations. As a result, the Server is assumed to offer services only for one Client at a time. However, the implementation may offer a possibility for multiple Clients at a time but this is not a requirement.

2.4 PROFILE FUNDAMENTALS

The profile fundamentals, with which all application profiles must comply, are the following:

1. Before a Server is used with a Client for the first time, a bonding procedure including the pairing may be performed (see Section 7.3.1). This procedure must be supported, but its usage is dependent on the application profiles. The bonding typically involves manually activating bonding support and entering a Bluetooth PIN code (see Section 7.3.1) on the keyboards of the Client and Server devices. This procedure may have to be repeated under certain circumstances; for example, if a common link key (as a bonding result) is removed on the device involved in the object exchange.
2. In addition to the link level bonding, an OBEX initialization procedure may be performed (see Section 5.3) before the Client can use the Server for the first time. The application profiles using GOEP must specify whether this procedure must be supported to provide the required security level.
3. Security can be provided by authenticating the other party upon connection establishment, and by encrypting all user data on the link level. The authentication and encryption must be supported by the devices; but whether they are used depends on the application profile using GOEP.
4. Link and channel establishments must be done according to the procedures defined in GAP (see Section 7.1-7.2 in [14]). Link and channel establishment procedures in addition to the procedures in GAP must not defined by the application profiles using GOEP.
5. There are no fixed master/slave roles.
6. This profile does not require any lower power mode to be used.

3 USER INTERFACE ASPECTS

User interface aspects are not defined in this profile.They are instead defined in the application profiles, where necessary.

4 APPLICATION LAYER

This section describes the service capabilities which can be utilized by the application profiles using GOEP.

4.1 FEATURE OVERVIEW

Table 4.1 shows the features which the Generic Object Exchange profile provides for the application profiles. The usage of other features (e.g. setting the current directory) must be defined by the applications profiles needing them.

Feature no.	Feature
1	Establishing an Object Exchange session
2	Pushing a data object
3	Pulling adata object

Table 4.1: Features provided by GOEP

4.2 ESTABLISHING AN OBJECT EXCHANGE SESSION

This feature is used to establish the object exchange session between the Client and Server. Before a session is established, payload data cannot be exchanged between the Client and the Server. The usage of the OBEX operations for establishing an OBEX session is described in Section 5.4.

4.3 PUSHING A DATA OBJECT

If data needs to be transferred from the Client to the Server, then this feature is used. The usage of the OBEX operations for pushing the data object(s) is described in Section 5.5.

4.4 PULLING A DATA OBJECT

If data need to be transferred from the Server to the Client, then this feature is used. The usage of the OBEX operations for pulling the data object(s) is described in Section 5.6.

5 OBEX INTEROPERABILITY REQUIREMENTS

5.1 OBEX OPERATIONS USED

Table 5.1 shows the OBEX operations which are specified by the OBEX protocol. The application profiles using GOEP must specify which operations must be supported to provide the functionality defined in the application profiles.

Operation no.	OBEX Operation
1	Connect
2	Disconnect
3	Put
4	Get
5	Abort
6	SetPath

Table 5.1: OBEX Operations

The IrOBEX specification does not define how long a client should wait for a response to an OBEX request. However, implementations which do not provide a user interface for canceling an OBEX operation should wait a reasonable period between a request and response before automatically canceling the operation. A reasonable time period is 30 seconds or more.

5.2 OBEX HEADERS

Table 5.2 shows the specified OBEX headers.

Header no.	OBEX Headers
1	Count
2	Name
3	Type
4	Length
5	Time
6	Description
7	Target
8	HTTP

Table 5.2: OBEX Headers

Header no.	OBEX Headers
9	Body
10	End of Body
11	Who
12	Connection ID
13	Authenticate Challenge
14	Authenticate Response
15	Application Parameters
16	Object Class

Table 5.2: OBEX Headers

Applications profiles dedicated to specific usage models must specify which of these headers must be supported.

5.3 INITIALIZATION OF OBEX

If the OBEX authentication is supported and used by the Server and the Client, the initialization for this authentication (see also Section 5.4.2) must be done before the first OBEX connection can be established. The initialization can be done at any time before the first OBEX connection. The initialization of the OBEX authentication requires user intervention on both the Client device and the Server device.

Authentication is done using an OBEX password, which may be the same as a Bluetooth PIN code on the link level. Even if the user uses the same code for link authentication and OBEX authentication, the user must enter these codes separately. After entering the OBEX password in both the Client and Server, the OBEX password is stored in the Client and the Server, and it can be used in the future for authenticating the Client and the Server. When an OBEX connection is established, the devices must authenticate each other if the OBEX authentication is enabled.

5.4 ESTABLISHMENT OF OBEX SESSION

For the Object Exchange, the OBEX connection can be made with or without OBEX authentication. In the next two subsections, both of these cases are explained. All application profiles using GOEP must support an OBEX session without authentication.

5.4.1 OBEX Session without Authentication

Figure 5.1 depicts how an OBEX session is established using the CONNECT operation.

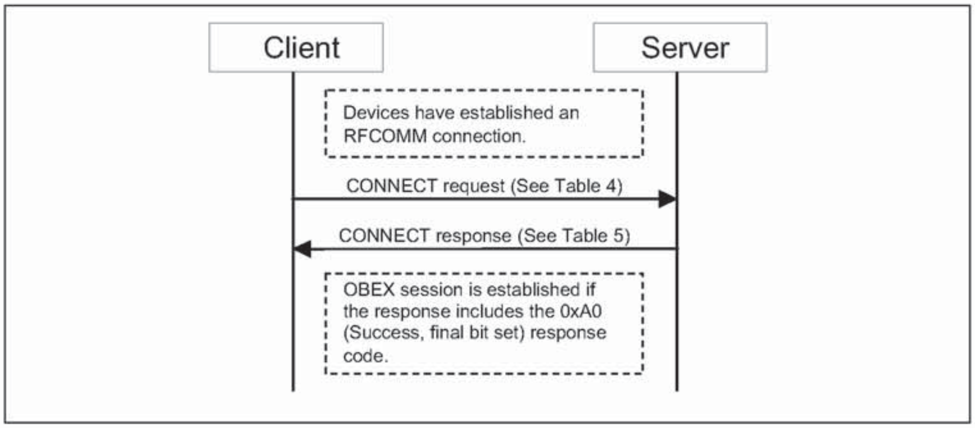
Client
Server
Devices have established an RFCOMM connection.
CONNECT request (See Table 4)
CONNECT response (See Table 5)
OBEX session is established if the response includes the 0xA0 (Success, final bit set) response code.

Figure 5.1: Establishment of OBEX Session without Authentication

The CONNECT request indicates a need for connection and may also indicate which service is used. The fields in the CONNECT request are listed below:

Field/ Header	Name	Value	Status	Explanation
Field	Opcode for CONNECT	0x80	M	-
Field	Connect Packet Length	Varies	M	-
Field	OBEX Version Number	Varies	M	-
Field	Flags	Varies	M	-
Field	Max OBEX Packet Length	Varies	M	-
Header	Target	Varies	C1	Used to indicate the specific Service.

Table 5.3: Fields and Headers in CONNECT Request

C1: The use of the Target header is mandatory for some application profiles. The application profiles define explicitly whether they use it or not. For the Target header, the example value could be 'IRMC-SYNC' to indicate the IrMC synchronization service. The target header is placed after the Maximum OBEX Packet Length field in the CONNECT request.

The response to the CONNECT request includes the fields listed below:

Field/ Header	Name	Value	Status	Explanation
Field	Response code for CONNECT request	Varies	M	0xA0 for success
Field	Connect Response Packet Length	Varies	M	-
Field	OBEX Version Number	Varies	M	-
Field	Flags	Varies	M	-
Field	Max OBEX Packet Length	Varies	M	-
Header	ConnectionID	Varies	C2	The header value specifies the current connection to the specific service.
Header	Who	Varies	C2	The header value matches the Target header value.

Table 5.4: Fields and Headers in CONNECT Response

C2: The Who and Connection ID headers must be used if the Target header is used in the Connect request. These headers are placed after the Maximum OBEX Packet Length field in the response to the CONNECT request.

5.4.2 OBEX Session with Authentication

The OBEX authentication scheme is based on the HTTP scheme but does not have all the features and options. In GOEP, OBEX authentication is used to authenticate the Client and the Server. Figure 5.2 depicts establishment of an OBEX session with authentication.

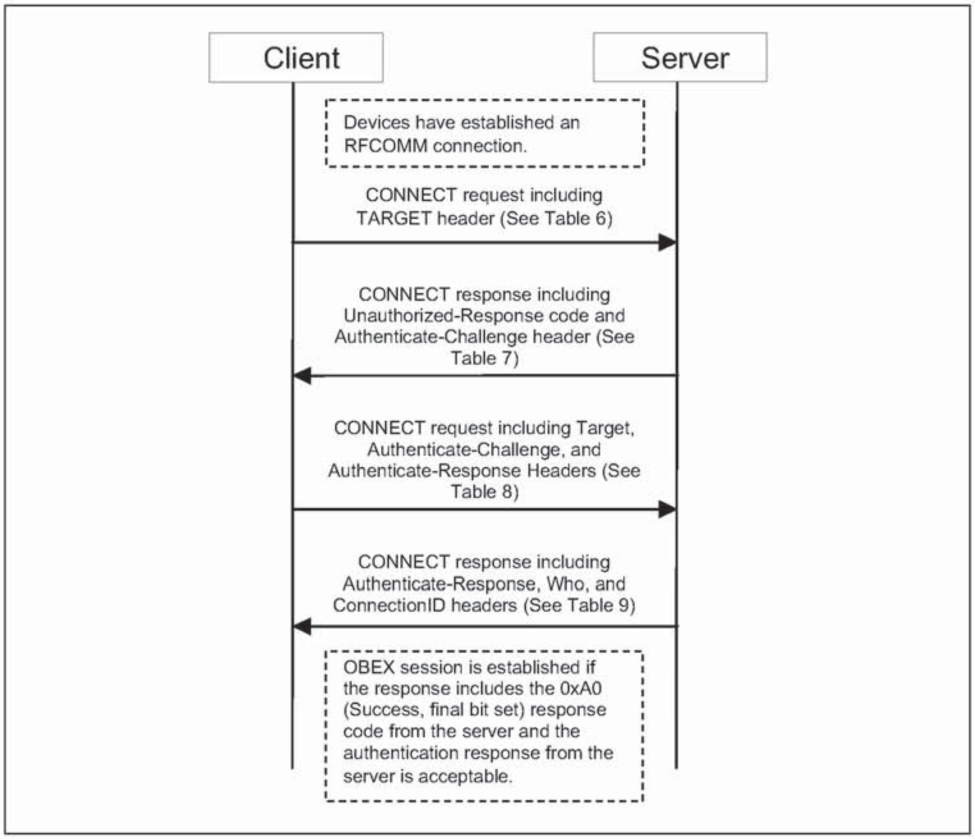
Client
Server
Devices have established an RFCOMM connection.
CONNECT request including TARGET header (See Table 6)
CONNECT response including Unauthorized-Response code and Authenticate-Challenge header (See Table 7)
CONNECT request including Target, Authenticate-Challenge, and Authenticate-Response Headers (See Table 8)
CONNECT response including Authenticate-Response, Who, and ConnectionID headers (See Table 9)
OBEX session is established if the response includes the 0xA0 (Success, final bit set) response code from the server and the authentication response from the server is acceptable.

Figure 5.2: Establishment of OBEX Session with Authentication

The first CONNECT request indicates a need for connection and which service is used. The fields and the header in the CONNECT request are listed below:

Field/ Header	Name	Value	Status	Explanation
Field	Opcode for CONNECT	0x80	M	-
Field	Connect Packet Length	Varies	M	-
Field	OBEX Version Number	Varies	M	-

Table 5.5: Fields and Headers in CONNECT Request when Authentication Used

Field/ Header	Name	Value	Status	Explanation
Field	Flags	Varies	M	-
Field	Max OBEX Packet Length	Varies	M	-
Header	Target	Varies	C1	Used to indicate the specific Service

Table 5.5: Fields and Headers in CONNECT Request when Authentication Used

C1: The usage of the Target header is dependent on the application profile utilizing GOEP. The example value for the Target header can be 'IRMC-SYNC' to indicate the IrMC synchronization service.

The first response to the CONNECT request from the Server, which authenticates the Client, includes the following fields and headers:

Field/ Header	Name	Value	Status	Explanation
Field	Response code for CONNECT request	Varies	M	0x41 for Unauthorized, because OBEX authentication is used.
Field	Connect Response Packet Length	Varies	M	-
Field	OBEX Version Number	Varies	M	-
Field	Flags	Varies	M	-
Field	Max OBEX Packet Length	Varies	M	-
Header	Authenticate Challenge	Varies	M	Carries the digest-challenge string.

Table 5.6: Fields and Headers in First CONNECT Response when Authenticating

The second CONNECT request has the following fields and headers in this order:

Field/ Header	Name	Value	Status	Explanation
Field	Opcode for CONNECT	0x80	M	-
Field	Connect Packet Length	Varies	M	-
Field	OBEX Version Number	Varies	M	-
Field	Flags	Varies	M	-
Field	Max OBEX Packet Length	Varies	M	-

Table 5.7: Fields and Headers in Second CONNECT Request when Authentication Used

Field/ Header	Name	Value	Status	Explanation
Header	Target	Varies	C1	-
Header	Authenticate Challenge	Varies	M	Carries the digest-challenge string.
Header	Authenticate Response	Varies	M	Carries the digest-response string. This is the response to the challenge from the Server.

Table 5.7: Fields and Headers in Second CONNECT Request when Authentication Used

C1: see Table 5.5

The second response to the CONNECT request has the following fields and headers:

Field/ Header	Name	Value	Status	Explanation
Field	Response code for CONNECT request	Varies	M	0xA0 for success
Field	Connect Response Packet Length	Varies	M	-
Field	OBEX Version Number	Varies	M	-
Field	Flags	Varies	M	-
Field	Max OBEX Packet Length	Varies	M	-
Header	ConnectionID	Varies	M	The header value specifies the current connection to the specific service.
Header	Who	Varies	M	The header value matches the Target header value.
Header	Authenticate Response	Varies	M	Carries the digest-response string. This is the response to the challenge from the Client.

Table 5.8: Fields and Headers in Second CONNECT Response when Authenticating

If the response code from the Server is successful, and the Client accepts the authentication response from the Server, the session is established and authenticated.

5.5 PUSHING DATA TO SERVER

The data object(s) is pushed to the Server using the PUT operation of the OBEX protocol. The data can be sent in one or more OBEX packets.
The PUT request must include the following fields and headers:

Field/ Header	Name	Value	Status	Explanation
Field	Opcode for PUT	0x02 or 0x82	M	-
Field	Packet Length	Varies	M	-
Header	ConnectionID	Varies	C1	The header value specifies the current connection to the specific service.
Header	Name	Varies	M	The header value is the name of a single object, object store, or log information.
Header	Body/End of Body	Varies	M	End of Body identifies the last chunk of the object body.

Table 5.9: Fields and Headers in PUT Request

C1: The ConnectionID header is mandatory if the Target header is used when establishing the OBEX session.

Other headers, which can be optionally used, are specified in [11].

The response packet for the PUT request has the following fields and headers:

Field/ Header	Name	Value	Status	Explanation
Field	Response code for PUT	0x90 or 0xAO	M	0x90 for continue or 0xA0 for success
Field	Packet Length	Varies	M	-

Table 5.10: Fields and Headers in PUT Response

Other headers, which can be optionally used, are specified in [11].

5.6 PULLING DATA FROM SERVER

The data object(s) is pulled from the Server using the GET operation of the OBEX protocol. The data can be sent in one or more OBEX packets. The first GET request includes the following fields and headers.

Field/ Header	Name	Value	Status	Explanation
Field	Opcode for GET	0x03	M	-
Field	Packet Length	Varies	M	-
Header	ConnectionID	Varies	C1	The header value specifies the current connection to the specific service.
Header	Type	Varies	C2	Indicates the type of the object to be pulled.
Header	Name	Varies	C2	The header value is the name of a single object, object store, or log information.

Table 5.11: Fields and Headers in GET Request

C1: The ConnectionID header is mandatory if the Target header is used when establishing the OBEX session.

C2: Either the Type header or the Name header must be included in the GET request when it is sent to the server.

Other headers, which can be optionally used, are specified in [11].

The response packet for the GET request has the following fields and headers:

Field/ Header	Name	Value	Status	Explanation
Field	Response code for Get	0x90 or 0xA0	M	0x90 or 0xA0 if the packet is the last the object
Field	Packet Length	Varies	M	-
Header	Name	Varies	O	The header value is the name of a single object, object store, or log information.
Header	Body/End of Body	Varies	M	End of Body identifies the last chunk of the object body.

Table 5.12: Fields and Headers in GET Response

Other headers, which can be optionally used, are specified in [11].

5.7 DISCONNECTION

see Chapter 2.2.2 in [1].

6 SERIAL PORT PROFILE INTEROPERABILITY REQUIREMENTS

This profile requires compliance to the protocol requirements of the Serial Port Profile (SeP) [12]. For the purposes of reading the SeP [12], the Server shall always be considered to be Device B and the Client shall always be considered to be Device A.

The following text, together with the associated sub-clauses, defines the requirements with regards to this profile – in addition to the requirements defined in [9].

6.1 RFCOMM INTEROPERABILITY REQUIREMENTS

For the RFCOMM layer, no additions to the requirements stated in Section 4 of Serial Port Profile apply.

6.2 L2CAP INTEROPERABILITY REQUIREMENTS

For the L2CAP layer, no additions to the requirements stated in Section 5 of Serial Port Profile apply.

6.3 SDP INTEROPERABILITY REQUIREMENTS

These requirements are defined by the application profiles. Thus, none of the requirements defined in the SeP profile (Section 6 in [12]) apply to this profile.

6.4 LINK MANAGER (LM) INTEROPERABILITY REQUIREMENTS

For the LM layer, no additions to the requirements stated in Section 7 of Serial Port Profile apply.

6.5 LINK CONTROL (LC) INTEROPERABILITY REQUIREMENTS

In the table below, LC capabilities differing from the capabilities required by the SeP profile (Section 8 in [12]) are listed.

	Capabilities	Support in baseband	Support in Server	Support in Client
5.	Packet types			
L	HV1 packet	M	X	X

Table 6.1: Baseband/LC capabilities

	Capabilities	Support in baseband	Support in Server	Support in Client
M	HV2 packet	O	X	X
N	HV3 packet	O	X	X
O	DV packet	M	X	X
7.	Voice codec			
A	A-law	O	X	X
B	μ-law	O	X	X
C	CVSD	O	X	X

Table 6.1: Baseband/LC capabilities

6.5.1 Inquiry and Inquiry Scan

For this profile, the Limited discoverable mode (see Section 7.1) should be used; but, if the Server device for some reason (e.g. lack of a sufficient user interface) wants to be visible at all times, the General discoverable mode (see Section 7.1) can be used instead. The client device must support the General inquiry procedure (see Section 7.3), and should also support the Limited inquiry procedure.

If the Limited inquiry procedure is supported, it should be used primarily. When this procedure is initiated in the Client, the client must perform this procedure for at least $T_{GAP}(100)$ (see Section 6.2.4 in GAP [14]). After the execution of the Limited inquiry procedure, the device may fall back to perform the General inquiry procedure. The device must support this fall-back functionality if the Limited inquiry procedure is supported. The fall-back procedure may or may not require user intervention. When general inquiry is initiated by the Client after limited inquiry, it shall be in this General limited procedure state for at least $T_{GAP}(100)$ (see Section 6.2.4 in GAP [14]).

For the inquiry, the returned CoD in the FHS packet must indicate that Object Transfer service is supported (see [13]). The major and minor device classes depend on the device supporting this profile. Therefore, usage of them is not defined in this profile.

The Limited Inquiry, Device Discovery and Name Discovery procedures are described in Section 6.2-6.4 in the Generic Access profile [14].

7 GENERIC ACCESS PROFILE INTEROPERABILITY REQUIREMENTS

This profile requires compliance to the Generic Access Profile. This section defines the support requirements with regards to procedures and capabilities defined in GAP.

7.1 MODES

Table 7.1 shows the support status for Modes within this profile.

	Procedure	Support in Client	Support in Server
1	Discoverability modes		
	Non-discoverable mode	N/A	M
	Limited discoverable mode	N/A	C1
	General discoverable mode	N/A	C1
2	Connectability modes		
	Non-connectable mode	N/A	O
	Connectable mode	N/A	M
3	Pairing modes		
	Non-pairable mode	N/A	M
	Pairable mode	N/A	M

Table 7.1: Modes

C1: The Limited discoverable mode should be used, but if the Server device for some reason (e.g. lack of a sufficient user interface) wants to be visible at all times, the General discoverable mode can be used instead.

7.2 SECURITY ASPECTS

Table 7.2 shows the support status for Security aspects within this profile.

	Procedure	Support in Client	Support in Server
1	Authentication	M	M
2	Security modes		

Table 7.2: Security aspects

	Procedure	Support in Client	Support in Server
	Security modes 1	M	M
	Security modes 2	C1	C1
	Security modes 3	C1	C1

Table 7.2: Security aspects

C1: Support for at least one of the security modes 2 and 3 is mandatory.

7.3 IDLE MODE PROCEDURES

Table 7.3 shows the support status for Idle mode procedures within this profile.

	Procedure	Support in Client	Support in Server
1	General inquiry	M	N/A
2	Limited inquiry	O	N/A
3	Name discovery	M	N/A
4	Device discovery	M	N/A
5	Bonding	M (Note 1)	M (Note 1)
Note 1: see section 7.3.1			

Table 7.3: Idle mode procedures

7.3.1 Bonding

It is mandatory for the Client and Server to support bonding. Bonding may be required before permitting communication between a Client and a Server. During bonding, the Client and Server are paired, which means that the Client and Server establish a security association (a common link key). This requires that an identical Bluetooth PIN code be entered on both the Client and Server devices.

The usage of bonding is optional for both Client and Server. The bonding procedures are defined in Section 6.5 in GAP [14].

8 REFERENCES

8.1 NORMATIVE REFERENCES

[1] Bluetooth Special Interest Group, IrDA Interoperability

[2] Bluetooth Special Interest Group, Synchronization Profile

[3] Bluetooth Special Interest Group, File Transfer Profile

[4] Bluetooth Special Interest Group, Object Push Profile

[5] Bluetooth Special Interest Group, Baseband Specification

[6] Bluetooth Special Interest Group, LMP Specification

[7] Bluetooth Special Interest Group, L2CAP Specification

[8] Bluetooth Special Interest Group, RFCOMM with TS 07.10", Specification of the Bluetooth System

[9] ETSI, TS 07.10, Version 6.3.0

[10] Bluetooth Special Interest Group, SDP Specification

[11] Infrared Data Association, IrDA Object Exchange Protocol (IrOBEX) with Published Errata, Version 1.2, April 1999

[12] Bluetooth Special Interest Group, Serial Port Profile

[13] Internet Assigned Numbers Authority, IANA Protocol/Number Assignments Directory (http://www.iana.org/numbers.html), May 1999.

[14] Bluetooth Special Interest Group, Generic Access Profile

Part K:11

OBJECT PUSH PROFILE

This application profile defines the application requirements for Bluetooth devices necessary for the support of the Object Push usage model. The requirements are expressed in terms of end-user services, and by defining the features and procedures that are required for interoperability between Bluetooth devices in the Object Push usage model.

CONTENTS

FOREWORD

This document, together with the Generic Object Exchange profile and the Generic Access profile, forms the Object Push usage model.

Interoperability between devices from different manufacturers is provided for a specific service and usage model if the devices conform to a Bluetooth SIG defined profile specification. A profile defines a selection of messages and procedures (generally termed *capabilities*) from the Bluetooth SIG specifications and gives an unambiguous description of the air interface for specified service(s) and usage model(s).

All defined features are process-mandatory. This means that if a feature is used, it is used in a specified manner. Whether the provision of a feature is mandatory or optional is stated separately for both sides of the Bluetooth air interface.

1 INTRODUCTION

1.1 SCOPE

The Object Push profile defines the requirements for the protocols and procedures that shall be used by the applications providing the Object Push usage model. This profile makes use of the Generic Object Exchange Profile (GOEP) [10] to define the interoperability requirements for the protocols needed by applications. The most common devices using these usage models can be notebook PCs, PDAs, and mobile phones.

The scenarios covered by this profile are the following:

- Usage of a Bluetooth device, e.g. a mobile phone to push an object to the inbox of another Bluetooth device. The object can for example be a business card or an appointment.
- Usage of a Bluetooth device; e.g. a mobile phone to pull a business card from another Bluetooth device.
- Usage of a Bluetooth device; e.g. a mobile phone to exchange business cards with another Bluetooth device. Exchange defined as a push of a business card followed by a pull of a business card.

1.2 BLUETOOTH PROFILE STRUCTURE

In Figure 1.1 Bluetooth Profiles, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure: a profile has dependencies on the profile(s) in which it is contained – directly and indirectly. For example, the Object Push profile is dependent on Generic Object Exchange, Serial Port, and Generic Access profiles.

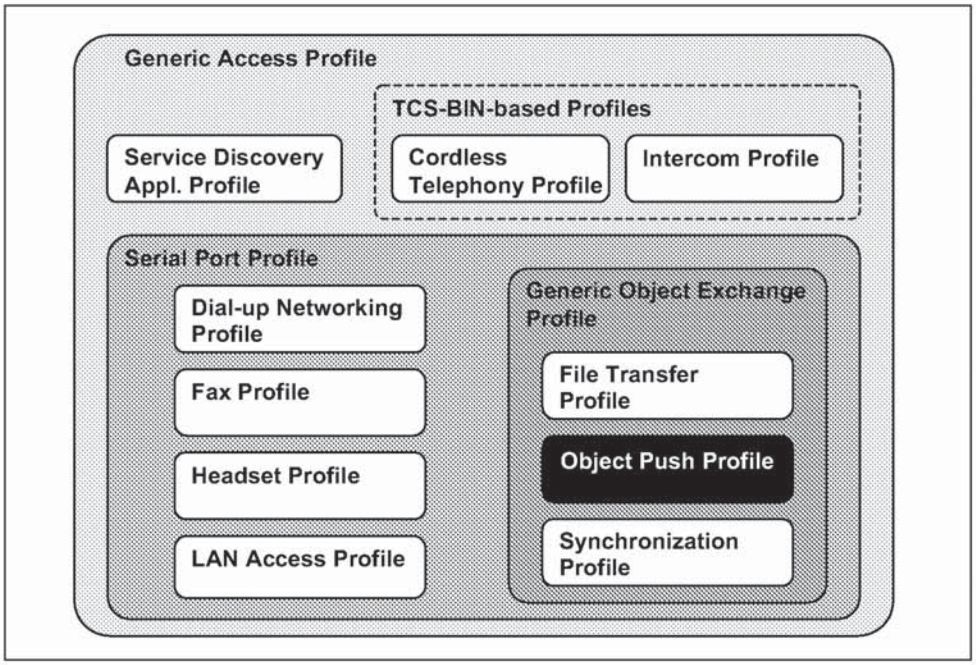

Figure 1.1: Bluetooth Profiles

1.3 BLUETOOTH OBEX-RELATED SPECIFICATIONS

Bluetooth Specification includes five separate specifications for OBEX and applications using OBEX.

1. Bluetooth IrDA Interoperability Specification [7].

- Defines how the applications can function over both Bluetooth and IrDA.
- Specifies how OBEX is mapped over RFCOMM and TCP.
- Defines the application profiles using OBEX over Bluetooth.

2. Bluetooth Generic Object Exchange Profile Specification [10]

- Generic interoperability specification for the application profiles using OBEX.
- Defines the interoperability requirements of the lower protocol layers (e.g. Baseband and LMP) for the application profiles.

3. Bluetooth Synchronization Profile Specification [15]

- Application Profile for Synchronization applications.
- Defines the interoperability requirements for the applications within the Synchronization application profile.
- Does not define the requirements for the Baseband, LMP, L2CAP, or RFCOMM.

4. Bluetooth File Transfer Profile Specification [14]

- Application Profile for File Transfer applications.
- Defines the interoperability requirements for the applications within the File Transfer application profile.
- Does not define the requirements for the Baseband, LMP, L2CAP, or RFCOMM.

5. **Bluetooth Object Push Profile Specification (this specification)**

- Application Profile for Object Push applications.
- Defines the interoperability requirements for the applications within the Object Push application profile.
- Does not define the requirements for the Baseband, LMP, L2CAP, or RFCOMM.

1.4 SYMBOLS AND CONVENTIONS

1.4.1 Requirement status symbols

In this document, the following symbols are used:

'M' for mandatory to support (used for capabilities that shall be used in the profile);

'O' for optional to support (used for capabilities that can be used in the profile);

'C' for conditional support (used for capabilities that shall be used in case a certain other capability is supported);

'X' for excluded (used for capabilities that may be supported by the unit but shall never be used in the profile);

'N/A' for not applicable (in the given context it is impossible to use this capability).

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices following this profile. Therefore, these features shall never be activated while a unit is operating as a unit within this profile.

1.4.2 Signaling diagram conventions

The following arrows are used in diagrams describing procedures:

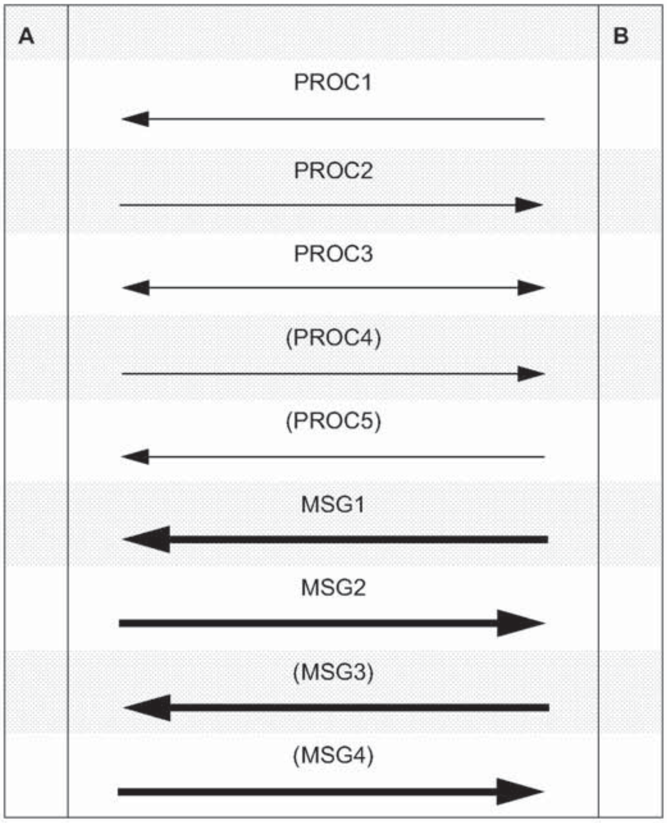

Table 1.1: Arrows used in signaling diagrams

In the table above, the following cases are shown: PROC1 is a sub-procedure initiated by B. PROC2 is a sub-procedure initiated by A. PROC3 is a sub-procedure where the initiating side is undefined (may be both A and B). PROC4 indicates an optional sub-procedure initiated by A, and PROC5 indicates an optional sub-procedure initiated by B.

MSG1 is a message sent from B to A. MSG2 is a message sent from A to B. MSG3 indicates an optional message from A to B, and MSG4 indicates an optional message from B to A.

2 PROFILE OVERVIEW

2.1 PROFILE STACK

The figure below shows the protocols and entities used in this profile.

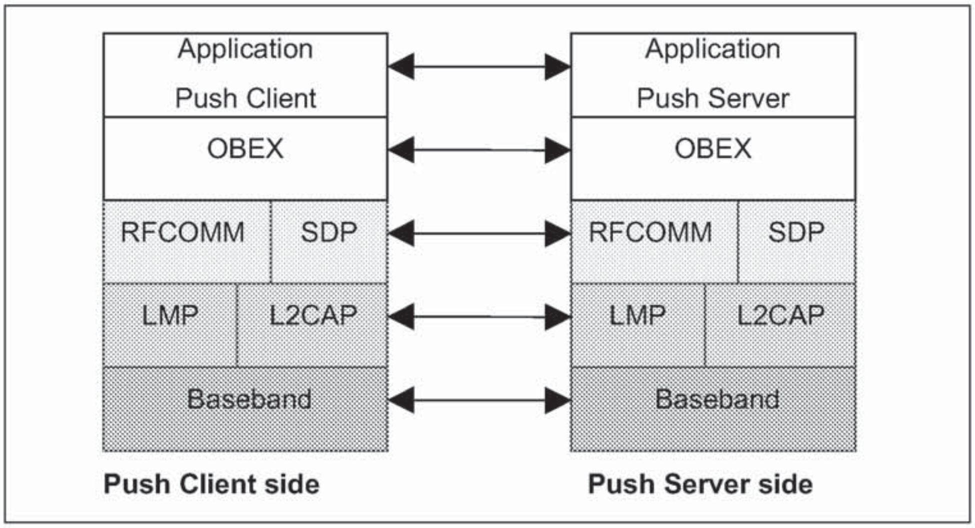

Figure 2.1: Protocol model

The Baseband [1], LMP [2] and L2CAP [3] are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM [4] is the Bluetooth adaptation of GSM TS 07.10 [5]. SDP is the Bluetooth Service Discovery Protocol [6]. OBEX [7] is the Bluetooth adaptation of IrOBEX [8].

The RFCOMM, L2CAP, LMP and Baseband interoperability requirements are defined in Section 6 in GOEP [10].

2.2 CONFIGURATIONS AND ROLES

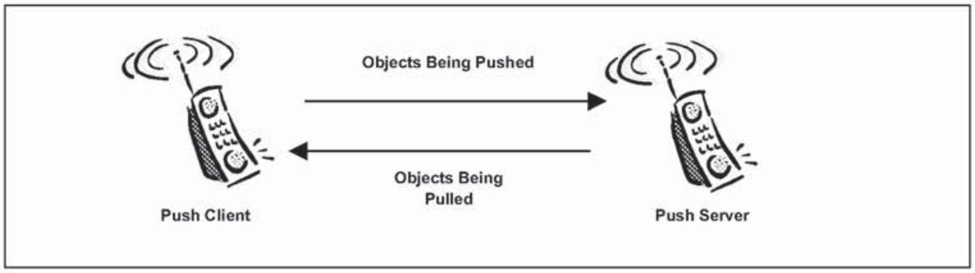

Figure 2.2: Push and Pull Example between two Mobile Phones

The following roles are defined for this profile:

Push Server – This is the server device that provides an object exchange server. In addition to the interoperability requirements defined in this profile, the Push Server must comply with the interoperability requirements for the server of the GOEP if not defined in the contrary.

Push Client – This is the client device that pushes and pulls objects to and from the Push Server. In addition to the interoperability requirements defined in this profile, the Push client must also comply with the interoperability requirements for the client of the GOEP, if not defined to the contrary.

2.3 USER REQUIREMENTS AND SCENARIOS

The scenarios covered by this profile are:

- Usage of a Push Client to push an object to a Push Server. The object can, for example, be a business card or an appointment.
- Usage of a Push Client to pull a business card from a Push Server.
- Usage of a Push Client to exchange business cards with a Push Server.

The restrictions applying to this profile are the same as in the GOEP.

The push operation described in this profile pushes objects from the Push Client to the inbox of the Push Server.

2.4 PROFILE FUNDAMENTALS

The profile fundamentals are the same as defined in the GOEP.

Link level authentication and encryption are mandatory to support and optional to use.

Bonding is mandatory to support and optional to use.

OBEX authentication is not used.

This profile does not mandate the server or client to enter any discoverable or connectable modes automatically, even if they are able to do so. On the Push Client side, end-user interaction is always needed to initiate the object push, business card pull or business card exchange.

3 USER INTERFACE ASPECTS

3.1 MODE SELECTION, PUSH SERVERS

Object Exchange mode affects the Push Server. It enables Push Clients to push and pull objects to and from the Push Server. The Push Clients can also try to pull objects from the Push Server in this mode. The Push Server does not have to support the pulling feature, but it must be able to respond with an appropriate error message.

When entering this mode, Push Servers should:
set the device in Limited Discoverable Mode (see Generic Access Profile),
must ensure that the Object Transfer bit is set in the CoD (see [16]),
and must ensure that a service record is registered in the SDDB (see Section 6).

Public devices, devices that want to be visible at all times, or devices that can not supply a user interface to enable Object Exchange mode shall use General Discoverable Mode (see [13]) instead of Limited Discoverable Mode.

It is recommended that this mode be set and unset by user interaction.

3.2 FUNCTION SELECTION, PUSH CLIENTS

- There are three different **functions** associated with the Object Push profile:
- Object Push function
- Business Card Pull function
- Business Card Exchange function

The **Object Push function** initiates the function that pushes one or more objects to a Push Server.

The **Business Card Pull function** initiates the function that pulls the business card from a Push Server.

The **Business Card Exchange function** initiates the function that exchanges business cards with a Push Server.

The three functions should be activated by the user. They should not be performed automatically without user interaction.

When the user selects one of these functions, an inquiry procedure will be performed to produce a list of available devices in the vicinity. Requirements on inquiry procedures are discussed in Section 6.5.1 of the GOEP [10].

3.3 APPLICATION USAGE EVENTS

In the following sections (3.3.1-3.3.3), the presented scenarios work as examples.Variations in the actual implementations are possible and allowed.

3.3.1 Object Push

When a Push Client wants to push an object to a Push Server, the following scenario can be followed. If authentication is used the user might have to enter a Bluetooth PIN at some point.

Push Client	Push Server
	The user sets the device **into Object Exchange mode**.
The user of the Push Client selects the **Object Push function** on the device.	
A list of Push Servers that may support the Object Push service is displayed to the user.	
The user selects a Push Server to push the object to. If the selected device does not support the Object Push service, the user is prompted to select another device.	
	When an object is received in the Push Server, it is recommended that the user of the Push Server be asked to accept or reject the object.
It is recommended that the user is notified of the result of the operation.	

3.3.2 Business Card Pull

When a Push Client wants to pull the business card from a Push Server the following user interaction can be followed.

If authentication is used, the user might have to enter a Bluetooth PIN at some point.

Push Client	Push Server
	The user sets the device into **Object Exchange mode**.
The user of the Push Client selects the **Business Card Pull function** on the device.	
A list of Push Servers that may support the Object Push service is displayed to the user.	
The user selects a Push Server to pull the business card from. If the selected device does not support the Object Push service, the user is prompted to select another device.	
	Some devices might ask the user whether or not to accept the request to pull the business card from his device.
It is recommended that the user is notified of the result of the operation.	

3.3.3 Business Card Exchange

When a Push Client wants to exchange business cards with a Push Server, the following user interaction can be followed.

If authentication is used, the user might have to enter a Bluetooth PIN at some point.

Push Client	Push Server
	The user sets the device into **Object Exchange mode**.
The user of the Push Client selects the **Business Card Exchange function** on the device.	
A list of Push Servers that may support the Object Push service is displayed to the user.	
The user selects a Push Server to exchange business cards with. If the selected device does not support the Object Push service, the user is prompted to select another device.	

Push Client	Push Server
	When a Push Client tries to exchange business cards with the Push Server, it is recommended that the user of the Push Server is asked to accept or reject the business card offered by the Push Client. Some devices might also ask the user whether or not to accept the request to pull the business card from his device.
It is recommended that the user is notified of the result of the operation.	

4 APPLICATION LAYER

This section describes the feature requirements on units active in the Object Push, Business Card Pull and Business Card Exchange use cases.

4.1 FEATURE OVERVIEW

Table 4.1 shows the features covered by the Object Push profile.

	Features	Support in Push Client	Support in Push Server
1.	Object Push	M	M
2.	Business Card Pull	O	O*
3.	Business Card Exchange	O	O*

Table 4.1: Application layer features

*. Optional, but the server must be able to respond with an error code on a pull request, even if it doesn't support this feature

4.2 OBJECT PUSH FEATURE

This feature lets a Push Client send one or more objects to a Push Server.

4.2.1 Content Formats

To achieve application level interoperability, content formats are defined for Object Push. For some applications content formats have been specified.

- Phone Book applications must support data exchange using the vCard 2.1 content format specified in [11]. The properties that are mandatory to support are listed in Chapter 7 of [9]. If a phone book application supports another content format it must still support the vCard 2.1 content format. If a device does not have a phone book application it does not have to support the vCard 2.1 content format.
- Calendar applications must support data exchange using the vCalendar 1.0 content format specified in [12]. The properties that are mandatory to support are listed in Chapter 8 of [9]. If a calendar application supports another content format it must still support the vCalendar 1.0 content format. If a device does not have a calendar application it does not have to support the vCalendar 1.0 content format.
- Messaging applications must support data exchange using the vMessage content format specified in Chapter 9 of [9]. If a messaging application supports another content format it must still support the vMessage content for-

mat as specified in Chapter 9 of [9]. If a device does not have a messaging application it does not have to support the vMessage content format.

- Notes applications must support data exchange using the vNote content format specified in Chapter 10 of [9]. If a notes application supports another content format it must still support the vNote content format as specified in Chapter 10 of [9]. If a device does not have a notes application it does not have to support the vNote content format.

It is highly recommended that a Push Client does not try to send objects of a format that the Push Server does not support. See Section 6 for information on how to find out which formats the Push Server supports.

The content formats supported by a Push Server must be identified in the SDDB.

4.2.2 Application Procedure

It is mandatory for Push Servers to be able to receive multiple objects within an OBEX connection. It is not mandatory for Push Clients to be able to send multiple objects during an OBEX connection. The Push Client uses one PUT operation for each object it wants to send. It is not mandatory to support sending or receiving of multiple objects within a single PUT operation.

Table 4.2 shows the application procedure required by the Push Client to push one or more objects to a Push Server.

Push Client	Details
OBEX CONNECT.	Target Header must not be used.
One or more OBEX PUTs for sending one or more objects.	
OBEX DISCONNECT	

Table 4.2: Application layer procedure for Object Push

For a detailed description of OBEX operations see Section 5.

4.3 BUSINESS CARD PULL FEATURE

A Push Client can optionally supply the functionality needed to pull a business card from a Push Server.

It is optional for the Push Server to support the business card pull feature. However, it must be able to respond to pull requests with an error message, see Section 5.6.

4.3.1 Owner's Business Card

Devices that support the business card pull and business card exchange services must store the owner's business card in the OBEX Default Get Object. Some devices (e.g. public devices) might hold information in the owner's business card that is relevant to the device rather than to the owner of the device.

The Default Get Object does not have a name; instead it is identified by its type. To achieve the ultimate application level interoperability, both the Push Client and the Push Server must support the vCard 2.1 content format specified in [11].

See [8] for a discussion on the Default Get Object.

4.3.2 Application Procedure Business Card Pull

Table 4.3 shows the application procedure required by the Push Client to perform a Business Card Pull from a Push Server.

Push Client	Details
OBEX CONNECT.	Target Header must not be used.
OBEX GET vCard of server's business card (default get object).	Type Header must be set to "text/x-vcard". Name Header must not be used.
OBEX DISCONNECT.	

Table 4.3: Application layer procedure for Business Card Pull

For a detailed description of OBEX operations see Section 5.

4.4 BUSINESS CARD EXCHANGE FEATURE

A Push Client can optionally supply the functionality needed to exchange business cards with a Push Server.

It is optional for the Push Server to support the business card exchange feature. It must, however, be able to respond to exchange requests with an error message, see Section 5.6.

4.4.1 Owner's Business Card

See Business Card Pull feature.

4.4.2 Application Procedure Business Card Exchange

Table 4.4 shows the application procedure required by the Push Client to perform a Business Card Exchange with a Push Server.

Push Client	Details
OBEX CONNECT.	Target Header must not be used.
OBEX PUT vCard with client's business card.	
OBEX GET vCard of server's business card (default get object).	Type Header must be set to "text/x-vcard". Name Header must not be used.
OBEX DISCONNECT.	

Table 4.4: Application layer procedure for Business Card Exchange

For a detailed description of OBEX operations see Section 5.

5 OBEX

5.1 OBEX OPERATIONS USED

Table 5.1 shows the OBEX operations, which are required in the Object Push profile.

Operation no.	OBEX Operation	Push Client	Push Server
1	Connect	M	M
2	Disconnect	M	M
3	Put	M	M
4	Get	O	M
5	Abort	M	M

Table 5.1: OBEX Operations

5.2 OBEX HEADERS

5.2.1 OBEX Headers for the Object Push Feature

Table 5.2 shows the specified OBEX headers which are required in the Object Push profile for the Object Push feature.

Header no.	OBEX Headers	Push Client	Push Server
1	Count	X	X
2	Name	M	M
3	Type	O	O
4	Length	M	M
5	Time	O	O
6	Description	O	O
7	Target	X	X
8	HTTP	O	O
9	Body	M	M
10	End of Body	M	M

Table 5.2: OBEX Headers used for the Object Push feature

Header no.	OBEX Headers	Push Client	Push Server
11	Who	X	X
12	Connection ID	X	X
13	Authenticate Challenge	X	X
14	Authenticate Response	X	X
15	Application Parameters	X	X
16	Object Class	X	X

Table 5.2: OBEX Headers used for the Object Push feature

5.2.2 OBEX Headers for the Business Card Pull and Exchange Features

Table 5.3 shows the specified OBEX headers which are required in the Object Push profile for the Business Card Pull and Exchange features.

Header no.	OBEX Headers	Push Client	Push Server
1	Count	X	X
2	Name	M	M
3	Type	M	M
4	Length	M	M
5	Time	O	O
6	Description	O	O
7	Target	X	X
8	HTTP	O	O
9	Body	M	M
10	End of Body	M	M
11	Who	X	X
12	Connection ID	X	X
13	Authenticate Challenge	X	X
14	Authenticate Response	X	X
15	Application Parameters	X	X
16	Object Class	X	X

Table 5.3: OBEX Headers used for the business card pull and business card exchange features

5.3 INITIALIZATION OF OBEX

Since OBEX authentication is not used by this profile, OBEX initialization is not applicable.

5.4 ESTABLISHMENT OF OBEX SESSION

See Section 5.4.1, in GOEP for a description of OBEX connection establishment without authentication.

The Push Client does not use the target header when establishing an OBEX connection.

5.5 PUSHING DATA

It is highly recommended that the Push Client use the Type Header when pushing objects to the Push Server.

See Section 5.5 in GOEP.

5.6 PULLING DATA

In the Object Push Profile, the Push Client only pulls data from the Push Server when it is getting the Default Get Object (owner's business card).

If there is no Default Get Object, the Push Server must respond with the error response code "NOT FOUND" [8]. The Push Client must be able to understand this error response code.

The Push Client must use the Type Header when getting the Default Get Object from the Push Server.

The Name Header is not used when getting the Default Get Object from the Push Server. If the Push Client sends a non-empty Name header, the Push Server should respond with the response code "FORBIDDEN"[8].

See Section 5.6 in GOEP.

5.7 DISCONNECTION

See Section 5.7 in GOEP.

6 SERVICE DISCOVERY

6.1 SD SERVICE RECORDS

The SD service record for the Object Push service is defined in Table 6.1. A Push Client does not provide any SD service records.

Item	Definition	Type Size	Value*	AttrID	Status	Default Value
Service Class ID List				See [16]	M	
Service Class #0		UUID	OBEXObjectPush		M	
Protocol Descriptor List				See [16]	M	
Protocol ID #0		UUID	L2CAP		M	
Protocol ID #1		UUID	RFCOMM		M	
Param #0	Channel	Uint8	Varies		M	
Protocol ID #2		UUID	OBEX		M	
Service Name	Displayable Text name	String	Varies	See [16]	O	"OBEX Object Push"
BluetoothProfileDescriptorList				See [16]	O	
Profile ID #0	Supported profile	UUID	OBEXObjectPush			OBEX-Object-Push [16]
Version #0	Profile version	uint16	Varies			0x0100
Supported Formats List	Supported Formats List	Data Element Sequence of Uint8	Formats: **0x01** = vCard 2.1 **0x02** = vCard 3.0 **0x03** = vCal 1.0 **0x04** = iCal 2.0 **0x05** = vNote (as defined in [9]) **0x06** = vMessage (as defined in [9]) **0xFF** = any type of object.	See [16]	M	

Table 6.1: Object Push Service Record

*. Values that are of the type UUID are defined in the Assigned Numbers specification [16].

6.2 SDP PROTOCOL DATA UNITS

Table 6.2 shows the specified SDP PDUs (Protocol Data Units), which are required in the Object Push profile.

PDU no.	SDP PDU	Push Client	Push Server
1	SdpErrorResponse	M	M
2	SdpServiceSearchAttributeRequest	M	M
3	SdpServiceSearchAttributeResponse	M	M

Table 6.2: SDP PDUs

7 REFERENCES

7.1 NORMATIVE REFERENCES

[1] Bluetooth Special Interest Group, Baseband Specification

[2] Bluetooth Special Interest Group, LMP Specification

[3] Bluetooth Special Interest Group, L2CAP Specification

[4] Bluetooth Special Interest Group, RFCOMM with TS 07.10

[5] ETSI, TS 07.10, Version 6.3

[6] Bluetooth Special Interest Group, SDP Specification

[7] Bluetooth Special Interest Group, IrDA Interoperability

[8] Infrared Data Association, IrDA Object Exchange Protocol (IrOBEX), Version 1.2 with Published Errata, April 1999

[9] Infrared Data Association, IrMC (Ir Mobile Communications) Specification with Published Errata, Version 1.1, February 1999

[10] Bluetooth Special Interest Group, Generic Object Exchange Profile

[11] The Internet Mail Consortium, vCard – The Electronic Business Card Exchange Format, Version 2.1, September 1996

[12] The Internet Mail Consortium, vCalendar – The Electronic Calendaring and Scheduling Exchange Format, Version 1.0, September 1996

[13] Bluetooth Special Interest Group, Generic Access Profile Specification

[14] Bluetooth Special Interest Group, File Transfer Profile Specification

[15] Bluetooth Special Interest Group, Synchronization Profile Specification

[16] Bluetooth Special Interest Group, Assigned Numbers specification

Part K:12

FILE TRANSFER PROFILE

This application profile defines the application requirements for Bluetooth devices necessary for the support of the File Transfer usage model. The requirements are expressed in terms of end-user services, and by defining the features and procedures that are required for interoperability between Bluetooth devices in the File Transfer usage model.

CONTENTS